Tivoli Public Key Infrastructure

Benutzerhandbuch

Version 3 Release 7.1

SH12-2978-02

Tivoli Public Key Infrastructure

Benutzerhandbuch

Version 3 Release 7.1

SH12-2978-02

Copyrightvermerke

Copyright © 1999, 2001 IBM Corp., einschließlich dieser Dokumentation und aller Software. Alle Rechte vorbehalten. Kann nur gemäß der Softwarelizenzvereinbarung von Tivoli Systems bzw. IBM oder dem Anhang für Tivoli-Produkte der IBM Nutzungsbedingungen verwendet werden. Diese Veröffentlichung darf ohne vorherige schriftliche Genehmigung der IBM Corp. weder ganz noch in Auszügen auf irgendeine Weise - elektronisch, mechanisch, magnetisch, optisch, chemisch, manuell u. a. - vervielfältigt, übertragen, aufgezeichnet, auf einem Abrufsystem gespeichert oder in eine andere Computersprache übersetzt werden. Die IBM Corp. gestattet Ihnen in begrenztem Umfang, eine Hardcopy oder eine Reproduktion einer maschinenlesbaren Dokumentation für den eigenen Gebrauch zu erstellen, unter der Voraussetzung, dass jede dieser Reproduktionen mit dem Copyrightvermerk der IBM Corp. versehen ist. Weitere das Copyright betreffende Rechte werden nur nach vorheriger schriftlicher Genehmigung durch die IBM Corp. gewährt. Die Veröffentlichung dient nicht zu Produktionszwecken. **Die in diesem Dokument aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.**

Marken

AIX, DB2, DB2 Universal Database, IBM, RS/6000, SecureWay, Tivoli and WebSphere sind in gewissen Ländern eingetragene Marken der International Business Machines Corp. oder von Tivoli Systems Inc.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von IBM WebSphere Application Server und IBM HTTP Web Server (″IBM Server″). Diese dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server (″IBM Server″). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Inhaltsverzeichnis

Vorwort ..... **vii**

Zielgruppe vii

Referenzinformationen vii

Inhalt des Handbuchs viii

In diesem Handbuch verwendete Konventionen ix

Kundenunterstützung anfordern ix

Tivoli PKI - Webinformationen ix

Kapitel 1. Produktinformationen zu Tivoli PKI **1**

Kapitel 2. Übersicht **3**

Kapitel 3. Informationen zur Vorgehensweise... ..... **5**

Zugreifen auf die Webseite für die Registrierung 5

Registrieren über einen Browser 5

Anfordern eines Browserzertifikats 6

Registrieren von Servern oder Einheiten 7

Vorabregistrieren einer Person 9

Prüfen des Registrierungsstatus 11

Verwalten von Zertifikaten über einen Browser 11

Aussetzen eines Zertifikats 12

Erneuern eines Zertifikats 12

Widerrufen eines Zertifikats 13

Abbrechen aktiver Anforderungen 14

Arbeiten mit mehreren Zertifikaten 14

Ausgeben einer Schlüsselsicherungsanforderung 14

Ausgeben einer Schlüsselwiederherstellungsanforderung 15

Kapitel 4. Informationen zu... ..... **17**

Registrierung 17

Vorabregistrierung 17

Webbrowserunterstützung 18

Registrierung 18

Unternehmensregel 18

Registrierungsstellen 18

Registrierungsdatenbanken 19

Registrierungsdomänen 19

Registrierungssätze 19

Satzattribute 20
Zertifizierung 20
Zertifikatsaussteller 20
Zertifikatswiderrufslisten (CRL) 20
Verzeichnisse (Directory) 20
Registrierte Namen 20
Zertifikate 21
Browserzertifikate 21
CA-Zertifikate 21
Server- oder Einheitenzertifikate 22
Zertifikatserweiterungen 22
Gültigkeitsdauer von Zertifikaten 22
Erneuerbarkeit 22
Zugriff auf gesicherte Ressourcen 23
Zugriffssteuerung 23
Authentifizierung und Berechtigung 23
Digitale Unterschriften 23
Sicherung und Wiederherstellung von Schlüsseln 23

Kapitel 5. Referenzinformationen 25

Registrierungsformular auf der Webseite 25
Gelieferte Zertifikatstypen 28
Gründe für das Widerrufen eines Zertifikats 29
Systemvoraussetzungen für die Browserregistrierung 30
Informationen zur Unterstützung in der Landessprache 30

Glossar 33

Index 53

Vorwort

Dieses Buch enthält Informationen darüber, wie Zertifikate abgerufen und verwaltet werden. Es beschreibt die Prozeduren zur Verwendung der Browserregistrierungsformulare von Tivoli PKI, um Zertifikate anzufordern, zu erneuern und zu widerrufen. Außerdem enthält es eine Erläuterung zur Vorabregistrierung für PKIX-kompatible Zertifikate.

Dieses Release des Produkts unterstützt lediglich AIX-Plattformen. Alle Materialien, die sich mit Microsoft Windows befassen, sollten ignoriert werden.

Zielgruppe

Dieses Buch richtet sich an Benutzer, die die browser-basierten Tivoli PKI-Funktionen benötigen, um eine Registrierungsanforderung zu übergeben oder um ein bereits vorhandenes, von Tivoli PKI ausgestelltes Zertifikat zu verwalten.

Benutzer dieses Handbuchs sollten sich in der Verwendung der unterstützten Internetbrowser auskennen und über Erfahrung mit e-business-Anwendungen verfügen.

Referenzinformationen

Die Tivoli PKI-Produktdokumentation steht im PDF- (Portable Document Format) sowie im HTML-Format auf der Tivoli-Website zur Verfügung. Die HTML-Versionen einiger Veröffentlichungen sind mit dem Produkt installiert und können über die Benutzerschnittstelle abgerufen werden.

Bitte beachten Sie, dass das Produkt seit Erstellung der Veröffentlichungen möglicherweise geändert worden ist. Die neuesten Produktinformationen sowie Informationen für den Zugriff auf Veröffentlichungen in den von Ihnen gewünschten Sprachen und Formaten enthalten die Release-Informationen. Die neueste Version der Release-Informationen steht auf der Tivoli Public Key Infrastructure-Website zur Verfügung:

`http://www.tivoli.com/support`

Zur Tivoli PKI-Bibliothek gehört die folgende Dokumentation:

Einführung
: Dieses Buch bietet eine Übersicht über das Produkt. Es enthält die Produktvoraussetzungen, beschreibt die Installationsverfahren und stellt Informationen darüber zur Verfügung, wie Sie auf die Onlinehilfefunktion für die jeweiligen Produktkomponenten zugreifen können. Dieses Buch liegt in gedruckter Form vor und wird mit dem Produkt geliefert.

Systemverwaltung
: Dieses Buch bietet allgemeine Informationen zur Verwaltung des Tivoli PKI-Systems. Es beschreibt die Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zur Verwaltung der Server-Komponenten sowie zum Erstellen von Protokollen und zur Ausführung von Datenintegritätsüberprüfungen.

Konfiguration
Dieses Buch enthält Informationen darüber, wie ein Tivoli PKI-System mit Hilfe des Konfigurationsassistenten (Setup Wizard) konfiguriert wird. Während Sie die Onlinehilfefunktion für den Assistenten anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

RA Desktop
Dieses Buch enthält Informationen darüber, wie Zertifikate im gesamten Zertifikatsverarbeitungszyklus mit Hilfe von RA Desktop verwaltet werden. Während Sie die Onlinehilfefunktion für den Desktop anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

Benutzerhandbuch
Dieses Buch enthält Informationen darüber, wie Zertifikate abgerufen und verwaltet werden. Es beschreibt die Prozeduren zur Verwendung der Browser-Registrierungsformulare von Tivoli PKI, um Zertifikate anzufordern, zu erneuern und zu widerrufen. Außerdem enthält es eine Erläuterung zur Vorabregistrierung bei PKIX-kompatiblen Zertifikaten.

Anpassung
Dieses Buch zeigt, wie die Tivoli PKI-Registrierungsfunktion angepasst wird, um die Vorgaben zur Registrierung und Zertifizierung im Rahmen Ihrer Unternehmensregeln zu unterstützen. So erhalten Sie beispielsweise Anweisungen zur Anpassung von HTML- und Java Server-Seiten, Benachrichtigungsschreiben, Zertifikatsprofilen und Regel-Exits.

Inhalt des Handbuchs

Dieses Handbuch enthält folgende Informationen:

- „Produktinformationen zu Tivoli PKI” auf Seite 1 liefert eine kurze Beschreibung der Funktionen und des Leistungsspektrums von Tivoli PKI.
- „Übersicht” auf Seite 3 liefert eine Beschreibung des Prozesses bei der Registrierung von Zertifikaten.
- „Informationen zur Vorgehensweise...” auf Seite 5 enthält Task-orientierte Informationen und Anleitungen zur Registrierung bei Tivoli PKI und zur Verwaltung der dort abgerufenen Zertifikate.
- „Informationen zu...” auf Seite 17 enthält Basisinformationen zu Tivoli PKI und Konzepten, die mit der Zertifikatsregistrierung, dem Registrierungsprozess und dem Zugriff auf gesicherte Ressourcen in Zusammenhang stehen.
- „Referenzinformationen” auf Seite 25 enthält Feldbeschreibungen, Werte und Attribute, die auf der Webseite des Registrierungsformulars dargestellt werden.
- „Glossar” auf Seite 33 definiert die Termini und Abkürzungen, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt sind, sowie Termini, die von Bedeutung sein könnten.

In diesem Handbuch verwendete Konventionen

In diesem Handbuch werden für bestimmte Termini und Aktionen verschiedene Konventionen hinsichtlich des Schriftbilds verwendet. Die Schriftbilder haben folgende Bedeutung:

Schriftbild	Bedeutung
Fettdruck	Befehle, Schlüsselwörter, Markierungen und andere Informationen, die im genauen Wortlaut verwendet werden müssen, werden **fett** gedruckt.
Kursivdruck	Variablen, die angegeben werden müssen, sowie neue Termini werden *kursiv* gedruckt. Hervorgehobene Wörter und Ausdrücke werden ebenfalls *kursiv* gedruckt.
Monospace-Schrift	Codebeispiele, Ausgabe und Systemnachrichten werden in einer `Monospace-Schrift` gedruckt.

Kundenunterstützung anfordern

Wenn mit irgendeinem Tivoli-Produkt Probleme auftreten, können Sie über **http://www.support.tivoli.com** die Homepage der Tivoli-Unterstützung (Tivoli Support) aufrufen. Nachdem Sie eine Verbindung zum Kundenregistrierungsformular hergestellt und dieses übergeben haben, können Sie auf eine Reihe von Kundenunterstützungsservices auf dem Web zugreifen.

Kunden in Deutschland, Österreich oder der Schweiz können eine der folgenden Telefonnummern anrufen:

- Deutschland: **01805-00-1242**
- Österreich: **01-1706-6000**
- Schweiz: **0800-555454**

Ihre Meinung zu Tivoli-Produkten und der Tivoli-Dokumentation interessiert uns. Gerne nehmen wir Verbesserungsvorschläge Ihrerseits entgegen. Falls Sie Kommentare oder Anregungen zur vorliegenden Dokumentation haben, senden Sie uns bitten eine E-Mail an folgende Adresse: pubs@tivoli.com.

Tivoli PKI - Webinformationen

Kunden von Tivoli und IBM Tivoli finden Onlineinformationen zu allen Tivoli-Sicherheitsprodukten und Tivoli PKI.

Um wichtige Informationen über kurzfristigen Produktaktualisierungen oder Serviceinformationen zu Tivoli PKI abzurufen, beginnen Sie auf folgender Website: **http://www.tivoli.com/support/secure_download_bridge.html**

Informationen zum Produkt Tivoli Public Key Infrastructure erhalten Sie auf folgender Website: **http://www.tivoli.com/products/index/secureway_public_key/**

Informationen zu anderen Sicherheitsverwaltungsprodukten von Tivoli erhalten Sie unter folgender Webadresse: **http://www.tivoli.com/products/solutions/security/**

1

Produktinformationen zu Tivoli PKI

Tivoli Public Key Infrastructure (Tivoli PKI) stellt Anwendungen zur Verfügung, mit denen Benutzer authentifiziert werden können und die eine sichere Kommunikationgewährleisten.

- Das Produkt ermöglicht es Unternehmen, digitale Zertifikate in Übereinstimmungen mit ihren Regeln zur Registrierung und Zertifizierung auszustellen, zu veröffentlichen und zu verwalten.
- Die Unterstützung von Public Key Infrastructure für X.509 Version 3 (PKIX) und CDSA-Verschlüsselungsstandards (Common Data Security Architecture) ermöglicht die Interoperabilität zwischen Produkten verschiedener Hersteller.
- Mit Hilfe von digitalen Unterschriften und sicheren Protokollen ist es möglich, alle Parteien einer Transaktion zu authentifizieren.
- Optimale Flexibilität durch browser-basierte Registrierungsfunktionen.
- Die verschlüsselte Kommunikation und die sichere Speicherung von Registrierungsinformationen sorgen für ein hohes Maß an Vertraulichkeit.

Ein Tivoli PKI-System kann auf IBM AIX/6000- und Microsoft Windows NT-Server-Plattformen ausgeführt werden. Es bietet die folgenden Hauptfunktionen:

- Ein zuverlässiger Zertifikatsaussteller (CA) verwaltet den gesamten Verarbeitungszyklus der digitalen Zertifizierung. Um die Authentizität eines Zertifikats zu bestätigen, versieht der CA jedes ausgestellte Zertifikat mit einer digitalen Unterschrift. Er unterzeichnet auch Zertifikatswiderrufslisten (CRLs), um zu bestätigen, dass bestimmte Zertifikate gültig sind. Zur weiteren Sicherung seines Signierschlüssels können Sie kryptografische Hardware wie beispielsweise den IBM SecureWay 4758 PCI Cryptographic Coprocessor verwenden.
- Eine Registrierungsstelle (RA) führt die administrativen Tasks im Hintergrund der Benutzerregistrierung aus. Die RA stellt sicher, dass nur solche Zertifikate ausgestellt werden, die Ihre Geschäftstätigkeit unterstützen, und dass diese Zertifikate ausschließlich an berechtigte Benutzer ausgegeben werden. Die administrativen Tasks können von automatisierten Prozessen ausgeführt werden oder von Mitarbeitern, die entsprechende Entscheidungen treffen.
- Eine Webschnittstelle für die Registrierung vereinfacht das Abrufen von Zertifikaten für Browser, Server und andere Einheiten und Zwecke, z. B. VPN-Einheiten (VPN = Virtual Private Network), Smartcards und die sichere Übertragung von E-Mails.
- Eine Verwaltungsschnittstelle auf Webbasis, RA Desktop, ermöglicht es berechtigten Registrierern, Registrierungsanforderungen zu genehmigen oder zurückzuweisen und Zertifikate nach dem Ausstellen zu verwalten.

- Ein Protokollierungssubsystem berechnet für jeden Protokolleintrag einen Nachrichtenauthentifizierungscode (MAC, Message Authentication Code). Wenn die Protokolldaten geändert oder gelöscht werden, nachdem sie in die Protokolldatenbank geschrieben wurden, können Sie diesen Eingriff anhand des MAC feststellen.
- Regel-Exits und Geschäftsprozessobjekte (Business Process Objects, BPO) ermöglichen Anwendungsentwicklern die Anpassung der Registrierungsprozesse.
- Integrierte Unterstützung für eine Steuerkomponente zur Verschlüsselung. Damit Operationen im Rahmen der Kommunikation authentifiziert werden können, werden die Hauptkomponenten von Tivoli PKI mit einem werkseitig erstellten privaten Schlüssel unterzeichnet. Sicherheitsobjekte wie beispielsweise Schlüssel und MACs werden verschlüsselt und in geschützten Bereichen, den so genannten KeyStores (Schlüsselspeichern), aufbewahrt.
- Integrierte Unterstützung für IBM Directory. Das Directory speichert Informationen zu gültigen und widerrufenen Zertifikaten in einem LDAP-kompatiblen Format (LDAP = Lightweight Direct Access Protocol).
- Integrierte Unterstützung für IBM WebSphere Application Server und IBM HTTP Server. Der Web-Server arbeitet mit dem RA-Server zusammen, um Nachrichten zu verschlüsseln, Anforderungen zu authentifizieren und Zertifikate an den vorgesehenen Empfänger zu senden.
- Integrierte Unterstützung für IBM DB2® Universal Database.

2

Übersicht

Wenn die gesicherten Anwendungen eines Unternehmens durch Tivoli PKI geschützt werden, können ausschließlich Benutzer mit entsprechenden Berechtigungen auf diese Anwendungen zugreifen. Wer eine Berechtigung wie beispielsweise ein digitales Zertifikat benötigt, kann diese anfordern, indem er bestimmte Informationen zur Verfügung stellt. Die Daten in der Registrierungsanforderung stellen die Grundlage für die Entscheidung dar, ob die Anforderung genehmigt oder zurückgewiesen wird. Wenn eine Registrierungsanforderung genehmigt wird, bearbeitet die Tivoli PKI-Registrierungsstelle (Registration Authority, RA) die Anforderung und der Tivoli PKI- Zertifikatsaussteller (Certificate Authority, CA) stellt das Zertifikat aus. Die Datensätze der Registrierungsanforderungen und Zertifikate befinden sich in einer verschlüsselten Registrierungsdatenbank.

In einem Tivoli PKI-System erfolgt die Anforderung von Zertifikaten über die Tivoli PKI-Registrierungsformulare, die auf einer Webseite zur Verfügung stehen.

Mit Hilfe der Registrierungsformulare können Sie die für die Anforderung eines Zertifikats erforderlichen Informationen übergeben und später zum Formular zurückkehren, um die Antwort der Tivoli PKI-Registrierungsfunktion abzurufen. Sie können ein Browser-Zertifikat, ein Server-Zertifikat oder ein Einheitenzertifikat beantragen. Sie haben auch die Möglichkeit, sich für ein Zertifikat vorab registrieren zu lassen, das den Zugriff auf PKIX-kompatible Anwendungen ermöglicht. Sie haben ebenfalls die Möglichkeit, zur Registrierungs-Web-Seite zurückzukehren, um die von dort direkt empfangenen Zertifikate zu verwalten.

Das vorliegende Handbuch unterstützt Sie bei allen genannten Registrierungs-Tasks.

3

Informationen zur Vorgehensweise...

Die Abschnitte in diesem Kapitel enthalten Anweisungen zu jedem Schritt bei der Registrierung eines Zertifikats auf der Registrierungswebseite von Tivoli PKI sowie Anweisungen dazu, wie Sie diese Seite verwenden, um die dort abgerufenen Browserzertifikate zu verwalten.

Zugreifen auf die Webseite für die Registrierung

Um auf die Registrierungs-Web-Seite zuzugreifen, gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass Ihre Datenstation die im Abschnitt „Systemvoraussetzungen für die Browserregistrierung" auf Seite 30 aufgeführten Anforderungen erfüllt.
2. Rufen Sie die in Ihrem Unternehmen verwendete Website für den Zugriff auf die Webseite für die Registrierung ab. Die Website weist das folgende Format auf:

   `http://`*`MyPublicWebServer`*`/`*`MyDomain`*`/index.jsp`
3. Öffnen Sie Ihren Browser, und geben Sie die Website ein:
   - Wenn Sie Netscape verwenden, geben Sie die Website in das Textfenster bei **Adresse** ein.
   - Wenn Sie Internet Explorer verwenden, geben Sie sie ebenfalls bei **Adresse** in das Textfenster ein.
4. Drücken Sie die **Eingabetaste**.

   Die Registrierungs-Web-Seite von Tivoli PKI wird angezeigt. Bei einer Standardinstallation lautet der Name der Seite 'Identitätsnachweis - Verwaltung'.
5. Wenn Sie die Tivoli PKI-Registrierungsservices das erste Mal verwenden, klicken Sie auf **das Zertifikat für Ihren Server**.

   Mit diesem Zertifikat kann Ihr Browser Daten authentifizieren, die von den Registrierungsservices gesendet werden. Wenn Sie diese Services das nächste Mal verwenden, können Sie diesen Schritt übergehen.

Registrieren über einen Browser

In diesem Abschnitt wird beschrieben, wie Sie Ihren Web-Browser verwenden, um ein Zertifikat auf der Tivoli PKI-Registrierungsseite anzufordern.

Wenn Sie die Registrierungsservices das erste Mal verwenden, müssen Sie ein CA-Zertifikat für Ihren Web-Browser abrufen, bevor Sie fortfahren können. Anschließend können Sie die Seiten zur Registrierung wiederholt verwenden.

Abhängig davon, wie die Registrierungsfunktion für Ihr Unternehmen angepasst wurde, können die Prozeduren, die zum Abrufen eines gültigen Zertifikats ausgeführt werden müssen, unterschiedlich sein. Im folgenden werden die grundlegenden Schritte erklärt. Wenden Sie sich an den zuständigen Systemadministrator, um Informationen über die für Ihren Standort gültigen Prozeduren zu erhalten.

Anfordern eines Browserzertifikats

Um ein Browser-Zertifikat über Ihren Web-Browser abzurufen, gehen Sie folgendermaßen vor:

1. Nehmen Sie über Ihren Browser Zugriff auf die Registrierungs-Web-Seite.
2. Öffnen Sie über **Registrierungstyp** die Liste, und wählen Sie **Browser-Zertifikat aus.**
3. Wählen Sie über **Aktion** die Option **Registrieren** aus.
4. Klicken Sie auf **OK**.

   Das angeforderte Registrierungsformular wird angezeigt.
5. Befolgen Sie die Anweisungen auf der Web-Seite, um die Felder des Formulars auszufüllen. Im Abschnitt „Registrierungsformular auf der Webseite" auf Seite 25 werden die Felder beschrieben. Das Formular enthält die folgenden Abschnitte:
   - Einen Abschnitt für die **Registrierungsinformationen** mit Textfenstern, in die Sie die Informationen zu Ihrer Person eingeben.
   - Einen Abschnitt für die **Zertifikatsanforderungsinformationen** mit Textfenstern, in die Sie die Informationen über das gewünschte Zertifikat eingeben. Wenn Sie in die Kanneingabefelder des jeweiligen Abschnitts keine Werte eintragen, setzt Tivoli PKI Standardwerte ein, die dem von Ihnen angeforderten Zertifikatstyp zugeordnet sind.

   Bitte achten Sie insbesondere auf die folgenden Felder:

   Zertifikatstyp
   Wählen Sie die Art des Browser-Zertifikats aus, das Sie für Ihr Unternehmen abrufen sollen. Unter „Gelieferte Zertifikatstypen" auf Seite 28 werden die verschiedenen Zertifikatstypen beschrieben.

   CA-Zertifikat auf Browser installieren
   Klicken Sie hier, um ein entsprechendes CA-Zertifikat abzurufen, das mit dem Zertifikatstyp vereinbar ist. Wenn Sie diesen Knopf anklicken, wird das CA-Zertifikat sofort heruntergeladen.

   Mit diesem Zertifikat kann Ihr Browser Daten authentifizieren, die von Tivoli PKI gesendet werden. Wenn Sie aus irgendeinem Grund bereits über ein solches Zertifikat verfügen, benötigen Sie davon kein zweites.

   E-Mail-Adresse
   Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre E-Mail-Adresse angeben.

   E-Mail-Benachrichtigung
   Wählen Sie dieses Feld aus, wenn Sie per E-Mail über das Ergebnis Ihrer Anforderung benachrichtigt werden wollen.

   Identifikationsprüfungsantwort
   Stellen Sie sicher, dass Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Allgemeiner Name

Das Feld **Allgemeiner Name** enthält bereits Informationen, die Sie für **Vorname** und **Nachname** angeben. Wenn Sie die Einträge für den Vor- bzw. Nachnamen zu einem späteren Zeitpunkt ändern, werden diese Änderungen möglicherweise nicht automatisch für den allgemeinen Namen übernommen. Ist dies der Fall, müssen Sie das Feld **Allgemeiner Name** mit dem geänderten **Vornamen** und **Nachnamen** aktualisieren, bevor Sie das Registrierungsformular übergeben.

Domänenname

Geben Sie den Namen der Maschine an, auf der das Zertifikat installiert wird, falls sie mit der Verwendung des Zertifikats in Zusammenhang steht. Für Browser-Zertifikate ist dieses Feld wahlfrei. Verwenden Sie das Feld nur, wenn Sie dazu entsprechende Anweisungen erhalten haben.

6. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nachdem Tivoli PKI das Registrierungsformular erhalten hat, geschieht Folgendes:
   - Wenn das Formular Fehler enthält, werden diese Fehler angezeigt. Nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Registrierungsanforderung erneut übergeben**.
   - Wenn das Formular keine Fehler enthält, wird ihre Anforderungs-ID auf einer anderen Web-Seite angezeigt.

7. Sie sollten Ihre Anforderungs-ID auf jeden Fall notieren. Sie dient später zu Ihrer Identifizierung, damit Sie den Status der Anforderung überprüfen können und Ihr Zertifikat nach dessen Fertigstellung erhalten. Führen Sie einen der folgenden Schritte aus, wie auf der Web-Seite beschrieben:

   - Markieren Sie die Web-Seite mit einem Lesezeichen, damit Sie ohne Schwierigkeiten zu dieser Anzeige zurückkehren und den Status Ihres Zertifikats überprüfen können.
   - Notieren Sie die Anforderungs-ID, damit Sie diese angeben können, wenn Sie zurückkehren.
   - Warten Sie, bis Ihnen die Anforderungs-ID per E-Mail zugesandt wird.

Registrieren von Servern oder Einheiten

Alle Server und Einheiten, die Sie registrieren, müssen über spezifische Merkmale verfügen, die den Definitionen dieses Handbuchs entsprechen. Im Abschnitt „Server- oder Einheitenzertifikate” auf Seite 22 werden diese Merkmale beschrieben.

Um ein Server- oder Einheitenzertifikat über Ihren Web-Browser abzurufen, gehen Sie folgendermaßen vor:

1. Nehmen Sie über Ihren Browser Zugriff auf die Registrierungs-Web-Seite.
2. Öffnen Sie über **Registrierungstyp** die Liste, und wählen Sie **Server- oder Einheitenzertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Registrieren** aus.
4. Klicken Sie auf **OK**.

   Das angeforderte Registrierungsformular wird angezeigt.
5. Befolgen Sie die Anweisungen auf der Web-Seite, um die Felder des Formulars auszufüllen. Im Abschnitt „Registrierungsformular auf der Webseite” auf Seite 25 werden die Felder beschrieben. Das Formular enthält die folgenden Abschnitte:

- Einen Abschnitt für die **Registrierungsinformationen** mit Textfenstern, in die Sie die Informationen zu Ihrer Person eingeben.
- Einen Abschnitt für die **Zertifikatsanforderungsinformationen** mit Textfenstern, in die Sie die Informationen über das für den Server oder die Einheit gewünschte Zertifikat eingeben. Wenn Sie in die Kanneingabefelder des jeweiligen Abschnitts keine Werte eintragen, setzt Tivoli PKI Standardwerte ein, die dem von Ihnen angeforderten Zertifikatstyp zugeordnet sind.

Bitte achten Sie insbesondere auf die folgenden Felder:

Zertifikatstyp
Wählen Sie die Art des Server- oder Einheitenzertifikats aus, das Sie für Ihr Unternehmen anfordern sollen. Unter „Gelieferte Zertifikatstypen” auf Seite 28 werden die verschiedenen Zertifikatstypen beschrieben.

CA-Zertifikat in Datei sichern
Klicken Sie hier, um ein entsprechendes CA-Zertifikat abzurufen, das mit dem Zertifikatstyp vereinbar ist. Ihr Browser fordert Sie auf, einen Pfad einzugeben. Wenn Sie diesen Knopf anklicken, wird das CA-Zertifikat sofort heruntergeladen.

Mit diesem Zertifikat kann der Server oder die Einheit Daten authentifizieren, die von Tivoli PKI gesendet werden. Wenn Sie aus irgendeinem Grund bereits über ein solches Zertifikat verfügen, benötigen Sie davon kein zweites.

E-Mail-Adresse
Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, wenn Sie per E-Mail über das Ergebnis Ihrer Anforderung benachrichtigt werden wollen.

Identifikationsprüfungsantwort
Stellen Sie sicher, dass Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Allgemeiner Name
Das Feld **Allgemeiner Name** enthält bereits Informationen, die Sie für **Vorname** und **Nachname** angeben. Wenn Sie die Einträge für den Vor- bzw. Nachnamen zu einem späteren Zeitpunkt ändern, werden diese Änderungen möglicherweise nicht automatisch für den allgemeinen Namen übernommen. Ist dies der Fall, müssen Sie das Feld **Allgemeiner Name** mit dem geänderten **Vornamen** und **Nachnamen** aktualisieren, bevor Sie das Registrierungsformular übergeben.

Domänenname
Geben Sie den Namen der Maschine an, auf der das Zertifikat installiert wird, falls sie mit der Verwendung des Zertifikats in Zusammenhang steht. Für Server-Zertifikate ist dieses Feld wahlfrei. Wenn Sie es verwenden, identifizieren Sie die Maschine, auf der der Web-Server installiert ist. Der **Domänenname** ist für IPSec-Zertifikate erforderlich. Sie müssen die IPSec-Einheit identifizieren, auf der das Zertifikat installiert wird.

6. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nachdem Tivoli PKI das Registrierungsformular erhalten hat, geschieht Folgendes:

   - Wenn das Formular Fehler enthält, werden diese Fehler angezeigt. Nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Registrierungsanforderung erneut übergeben**.
   - Wenn das Formular keine Fehler enthält, wird ihre Anforderungs-ID auf einer anderen Web-Seite angezeigt.

7. Sie sollten Ihre Anforderungs-ID auf jeden Fall notieren. Sie dient später zu Ihrer Identifizierung, damit Sie den Status der Anforderung überprüfen können und Ihr Zertifikat nach dessen Fertigstellung erhalten. Führen Sie einen der folgenden Schritte aus, wie auf der Web-Seite beschrieben:

   - Markieren Sie die Web-Seite mit einem Lesezeichen, damit Sie ohne Schwierigkeiten zu dieser Anzeige zurückkehren und den Status Ihres Zertifikats überprüfen können.
   - Notieren Sie die Anforderungs-ID, damit Sie diese angeben können, wenn Sie zurückkehren.
   - Warten Sie, bis Ihnen die Anforderungs-ID per E-Mail zugesandt wird.

Vorabregistrieren einer Person

Sie können die Registrierungsservices verwenden, um sich selbst oder eine andere Person vorab für ein Zertifikat zu registrieren, mit dem auf eine PKIX-kompatible Anwendung zugegriffen werden kann.

Um eine Person über den Web-Browser vorab zu registrieren, gehen Sie folgendermaßen vor:

1. Nehmen Sie über Ihren Browser Zugriff auf die Registrierungs-Web-Seite.
2. Öffnen Sie über **Registrierungstyp** die die Liste, und wählen Sie **Vorabregistrierung von Zertifikaten** aus.
3. Wählen Sie über **Aktion** die Option **Registrieren** aus.
4. Klicken Sie auf **OK**.

   Das angeforderte Registrierungsformular wird angezeigt.

5. Befolgen Sie die Anweisungen auf der Web-Seite, um die Felder des Formulars auszufüllen. Im Abschnitt „Registrierungsformular auf der Webseite” auf Seite 25 werden die Felder beschrieben. Das Formular enthält die folgenden Abschnitte:

   - Einen Abschnitt für die **Registrierungsinformationen** mit Textfenstern, in die Sie die Informationen über die Person eingeben, die Sie vorab registrieren wollen. An dieser Stelle geben Sie auch einige Informationen ein, anhand deren Sie den Status Ihrer Anforderung überprüfen können.
   - Einen Abschnitt für die **Zertifikatsanforderungsinformationen** mit Textfenstern, in die Sie die Informationen über das gewünschte Zertifikat eingeben. Wenn Sie in die Kanneingabefelder des jeweiligen Abschnitts keine Werte eintragen, setzt Tivoli PKI Standardwerte ein, die dem von Ihnen angeforderten Zertifikatstyp zugeordnet sind.

Bitte achten Sie insbesondere auf die folgenden Felder:

Zertifikatstyp
Wählen Sie den Zertifikatstyp aus, den die Person, die Sie vorab registrieren, benötigt. Unter „Gelieferte Zertifikatstypen” auf Seite 28 werden die verschiedenen Zertifikatstypen beschrieben.

E-Mail-Adresse
Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre eigene E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, wenn Sie per E-Mail über das Ergebnis Ihrer Anforderung benachrichtigt werden wollen.

Identifikationsprüfungsantwort
Stellen Sie sicher, dass Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Allgemeiner Name
Das Feld **Allgemeiner Name** enthält bereits Informationen, die Sie für **Vorname** und **Nachname** angeben. Wenn Sie die Einträge für den Vor- bzw. Nachnamen zu einem späteren Zeitpunkt ändern, werden diese Änderungen möglicherweise nicht automatisch für den allgemeinen Namen übernommen. Ist dies der Fall, müssen Sie das Feld **Allgemeiner Name** mit dem geänderten **Vornamen** und **Nachnamen** aktualisieren, bevor Sie das Registrierungsformular übergeben.

Domänenname
Geben Sie den Namen der Maschine an, auf der das Zertifikat installiert wird, falls sie mit der Verwendung des Zertifikats in Zusammenhang steht. Für Vorabregistrierungszertifikate ist dieses Feld wahlfrei. Verwenden Sie das Feld nur, wenn Sie dazu entsprechende Anweisungen erhalten haben.

6. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nachdem Tivoli PKI das Registrierungsformular erhalten hat, geschieht Folgendes:

   - Wenn das Formular Fehler enthält, werden diese Fehler angezeigt. Nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Registrierungsanforderung erneut übergeben**.
   - Wenn das Formular keine Fehler enthält, wird ihre Anforderungs-ID auf einer anderen Web-Seite angezeigt.

7. Sie sollten Ihre Anforderungs-ID auf jeden Fall notieren. Sie dient später zu Ihrer Identifizierung, damit Sie den Status der Anforderung überprüfen können und Ihr Zertifikat nach dessen Fertigstellung erhalten. Führen Sie einen der folgenden Schritte aus, wie auf der Web-Seite beschrieben:

   - Markieren Sie die Web-Seite mit einem Lesezeichen, damit Sie ohne Schwierigkeiten zu dieser Anzeige zurückkehren und den Status Ihres Zertifikats überprüfen können.
   - Notieren Sie die Anforderungs-ID, damit Sie diese angeben können, wenn Sie zurückkehren.
   - Warten Sie, bis Ihnen die Anforderungs-ID per E-Mail zugesandt wird.

Prüfen des Registrierungsstatus

Um den Status Ihrer Registrierungsanforderung zu überprüfen, müssen Sie entweder zur der Web-Seite zurückkehren, die Sie während der Registrierung mit einem Lesezeichen markiert haben, oder die folgenden Schritte ausführen:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungstyp** den Typ der von Ihnen angeforderten Registrierung aus.
3. Wählen Sie über **Aktion** die Option **Status überprüfen** aus.
4. Klicken Sie auf **OK**.

   Die Anzeige enthält Felder, in denen Sie Ihre Identität authentifizieren müssen, bevor Sie Informationen über Ihre Anforderung abrufen können.
5. In die folgenden Felder müssen Informationen eingegeben werden:
   - Bei **Anforderungs-ID** geben Sie die Anforderungs-ID ein, die nach Übergabe des Registrierungsformulars angezeigt wurde.
   - Bei **Identifikationsprüfungsantwort** geben Sie dieselbe Identifikationsprüfungsantwort ein, die Sie im Registrierungsformular angegeben haben.
6. Klicken Sie auf **Registrierungsstatus überprüfen**.

   Eine Nachricht zeigt den aktuellen Status Ihrer Anforderung an.
   - Wenn Ihre Anforderung noch anstehend ist, können Sie später hierher zurückkehren und den Status erneut überprüfen.
   - Wenn Ihre Anforderung genehmigt wurde, wird mit dem Registrierungstyp festgelegt, was als Nächstes erfolgt.

     Browser-Zertifikat
     Das Browser-Zertifikat wird sofort auf Ihren Browser heruntergeladen.

     Server- oder Einheitenzertifikat
     Der Browser fordert Sie auf, ein Format auszuwählen und einen Pfad anzugeben. Anschließend wird das Server- oder Einheitenzertifikat zum Ziel des Pfads heruntergeladen.

     Vorabregistrierung von Zertifikaten
     Es werden Informationen angezeigt, die der zukünftige Zertifikatseigner benötigt, um das Zertifikat anzufordern: eine Transaktions-ID, ein Kennwort und die Website der Registrierungsstelle (RA), die die Anforderung genehmigt hat. Auf Grundlage dieser Informationen wird eine Vorabregistrierungsdatei erstellt, die für die Registrierung beim Administrator verwendet wird.

Verwalten von Zertifikaten über einen Browser

Auf der Registrierungs-Web-Seite können Sie ein Browser-Zertifikat, das Sie heruntergeladen haben, auch erneuern oder widerrufen. Gegebenenfalls können Sie das Zertifikat auch in den Wartestatus setzten, anstatt es permanent zu widerrufen. Dies gilt nicht für Zertifikate, für die Sie eine Vorabregistrierung vorgenommen haben.

Anmerkung: Wenn Sie eine Fehlernachricht erhalten, während Sie Zertifikate mit Hilfe von Microsoft Internet Explorer erneuern oder widerrufen, liegt dies unter Umständen daran, dass Sie keine SSL-Sitzung mit Client-Authentifizierung zum Web-

Server herstellen können. Um dieses Problem zu lösen, wählen Sie im Browser **Extras → Internetoptionen** aus. Wählen Sie im Fenster für die Einstellungen der Internet-Optionen die Registerkarte **Erweitert** aus, und klicken Sie anschließend auf den Knopf **Standards wiederherstellen**. Dadurch wird SSL Version 3.0 erneut aktiviert. Klicken Sie auf **OK**, und schließen Sie den Browser. Starten Sie Internet Explorer erneut, und versuchen Sie erneut, eine Verbindung zum Server herzustellen.

Aussetzen eines Zertifikats

Sie können Browserzertifikate aussetzen, die Sie direkt über die Webseite für die Registrierung abgerufen haben.

Um ein Zertifikat auszusetzen, gehen Sie folgendermaßen vor:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungstyp** die Option **Browserzertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Aussetzen** aus.
4. Klicken Sie auf **OK**.
   Die Anzeige enthält Informationen, die Sie und das Zertifikat identifizieren.
5. Überprüfen Sie die Informationen, um sicherzustellen, dass dies auch tatsächlich das Zertifikat ist, das Sie aussetzen wollen.
6. Klicken Sie auf **Zertifikat aussetzen**.

Anmerkung: Wenn Sie ein ausgesetztes Zertifikat reaktivieren wollen, müssen Sie sich diesbezüglich mit dem RA-Administrator in Verbindung setzen, bevor die Karenzzeit des Zertifikats abläuft. Nach Ablauf der Karenzzeit kann ein ausgesetztes Zertifikat nicht mehr reaktiviert werden.

Erneuern eines Zertifikats

Sie können Browser-Zertifikate erneuern, die Sie direkt über die Registrierungs-Web-Seite abgerufen haben.

Um ein Zertifikat zu erneuern, gehen Sie folgendermaßen vor:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungstyp** die Option **Browserzertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Erneuern** aus.
4. Klicken Sie auf **OK**.
   Ein Erneuerungsformular wird angezeigt.
5. Überprüfen Sie das Formular, um sicherzustellen, dass dies auch tatsächlich das Zertifikat ist, das Sie erneuern wollen.
6. Ändern Sie gegebenenfalls die Werte in den editierbaren Feldern. Im Abschnitt „Registrierungsformular auf der Webseite” auf Seite 25 werden die Felder beschrieben.

   E-Mail-Adresse
   Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, wenn Sie per E-Mail vom Ergebnis Ihrer Anforderung informiert werden wollen.

Identifikationsprüfungsfrage
Sie können die Frage ändern, die Ihnen gestellt wird, wenn Sie den Status Ihrer Anforderung überprüfen.

Identifikationsprüfungsantwort
Stellen Sie sicher, dass Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Für Internet Explorer
- Befolgen Sie die Anweisungen auf dem Formular, wenn Sie den Provider für Ihren Verschlüsselungsservice wechseln wollen.
- Entscheiden Sie, ob ein neuer Schlüsselsatz erstellt oder der vorhandene erneut verwendet werden soll. Soll ein neuer Schlüsselsatz erstellt werden, haben Sie die Möglichkeit, ihn selbst zu benennen.
- Wählen Sie **Zusätzliche Sicherheitsoptionen** aus, um gegebenenfalls weitere Sicherheitsmaßnahmen von Microsoft Internet Explorer anzufordern.

7. Klicken Sie auf **Zertifikat erneuern**.
8. Merken Sie sich Ihre Anforderungs-ID, wenn diese angezeigt wird, damit Sie später den Status der Anforderung überprüfen können. Im Abschnitt „Prüfen des Registrierungsstatus" auf Seite 11 wird beschrieben, wie Sie den Status Ihrer Anforderung überprüfen können.

Widerrufen eines Zertifikats

Sie können Browser-Zertifikate widerrufen, die Sie direkt über die Registrierungs-Web-Seite abgerufen haben.

Um ein Zertifikat zu widerrufen, gehen Sie folgendermaßen vor:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungstyp** die Option **Browserzertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Widerrufen** aus.
4. Klicken Sie auf **OK**.
   Es werden Informationen zur Identifizierung des Zertifikats angezeigt.
5. Überprüfen Sie die Informationen, um sicherzustellen, dass dies auch das Zertifikat ist, das Sie widerrufen wollen.
6. Bei **Begründung** wählen Sie einen Grund aus, warum Sie das Zertifikat widerrufen wollen. Im Abschnitt „Gründe für das Widerrufen eines Zertifikats" auf Seite 29 werden die zulässigen Gründe beschrieben.
7. Bei **Datum, ab dem das Zertifikat nicht mehr gültig ist** geben Sie an, wann das Zertifikat widerrufen werden soll. Wählen Sie entweder das aktuelle Datum oder ein Datum in der Vergangenheit aus. Wenn die Begründung mit einem Datum zusammenhängt, verwenden Sie dieses Datum. Beispiel: Wenn Sie glauben, dass Ihr Schlüssel beschädigt wurde, wählen Sie das Datum aus, an dem dies Ihrer Meinung nach passiert ist.
8. Klicken Sie auf **Zertifikat widerrufen**.

Abbrechen aktiver Anforderungen

Wenn Sie eine Anforderung übergeben, um ein Zertifikat zu erneuern, zu widerrufen oder auszusetzen, und versuchen, diese Anforderung nach der Übergabe abzubrechen, gibt der Browser eine Fehlernachricht mit dem Inhalt ″Dokument enthält keine Daten″ zurück. Des weiteren kann der Browser die Registrierungs-Web-Seite nicht erneut anzeigen.

Dieser Fehler kann auftreten, wenn der Browser die Anforderung an den RA-Server weiterleitet, bevor er Sie zur Vorlage eines Zertifikats für die Authentifizierung auffordert. Wenn das Zertifikat nicht zusammen mit der Anforderung übergeben wird, wird ein Fehler zurückgegeben. Dies stellt die normale Browser-Funktionsweise dar. In dieser Situation kann der Browser nicht identifizieren, welches Zertifikat abgebrochen werden soll, nachdem der Knopf **Abbrechen** angeklickt wurde.

Arbeiten mit mehreren Zertifikaten

Wenn Sie eine Anforderung übergeben, um ein Zertifikat zu erneuern, zu widerrufen oder auszusetzen, und dann zur Webseite für die Registrierung zurückkehren, um mit einem anderen Zertifikat zu arbeiten, ist die Bearbeitung eines anderen Zertifikats erst dann möglich, nachdem Sie den Browser verlassen und erneut gestartet haben. Dies stellt die normale Browser-Funktionsweise dar. Sie müssen das aktuelle Zertifikat zunächst aus dem Browser-Cache löschen, bevor Sie versuchen, ein weiteres Zertifikat zu bearbeiten.

Ebenso kann ein Zertifikat, nachdem es heruntergeladen wurde, nicht in derselben Browser-Sitzung erneuert oder widerrufen werden. Sie müssen den Browser beenden, bevor Sie versuchen, ein neu installiertes Zertifikat zu bearbeiten.

Ausgeben einer Schlüsselsicherungsanforderung

Sie haben die Möglichkeit, die Erstellung einer Sicherungskopie eines Zertifikats und des zugehörigen privaten Schlüssels anzufordern. Die als Eingabe für diese Anforderung verwendete PKCS #12-Datei wird erstellt, wenn Sie ein Zertifikat aus einem unterstützten Browser exportieren. Diese PKCS #12-Datei kann dann zu einem späteren Zeitpunkt durch Ausgabe einer Schlüsselwiederherstellungsanforderung abgerufen werden.

Um eine Schlüsselsicherungsanforderung auszugeben, gehen Sie wie folgt vor:

1. Rufen Sie die in Ihrem Unternehmen verwendete Website für den Zugriff auf die Webseite für die **Schlüsselsicherungsanforderung** ab. Die URL hat das folgende Format:
   `http://`*`MyPublicWebServer`*`/`*`MyDomain`*`/KeyBackup_Request.jsp`
2. Öffnen Sie Ihren Browser, und geben Sie die Website ein:
   - Wenn Sie Netscape verwenden, geben Sie die Website in das Textfenster bei **Adresse** ein.
   - Wenn Sie Internet Explorer verwenden, geben Sie sie ebenfalls bei **Adresse** in das Textfenster ein.
3. Drücken Sie die **Eingabetaste**.
   Die Webseite für die **Schlüsselsicherungsanforderung** von Tivoli PKI wird angezeigt.
4. Geben Sie bei **PKCS #12-Datei** den Pfad und Dateinamen ein oder klicken Sie auf **Durchsuchen**, um die exportierte PKCS #12-Datei anzugeben, die das zu sichernde Zertifikat enthält.

5. Geben Sie bei **Kennwort der PKCS #12-Datei** das Kennwort ein, das beim Erstellen dieser Datei angegeben wurde.
6. Klicken Sie auf **Schlüsselsicherungsanforderung übergeben**.

   Daraufhin wird eine Nachricht mit dem aktuellen Status Ihrer Anforderung angezeigt.

Ausgeben einer Schlüsselwiederherstellungsanforderung

Sie haben die Möglichkeit, eine Anforderung auszugeben, um ein Zertifikat und den zugehörigen privaten Schlüssel aus einer Sicherungskopie abzurufen, die zuvor mittels einer Schlüsselsicherungsanforderung erstellt wurde. Nach Genehmigung der Wiederherstellungsanforderung durch den RA-Administrator wird die PKCS #12-Datei zum Downloaden für Sie bereitgestellt. Das Kennwort für die Datei wird nicht zur Verfügung gestellt, da Sie es bereits kennen sollten. Der RA-Administrator kann jedoch die Attribute der Datei, einschließlich Kennwort, anzeigen, falls der Antragsteller diese Informationen benötigt. Der Mechanismus für die Bereitstellung solcher Informationen wird normalerweise durch das Unternehmen definiert (beispielsweise E-Mail oder ein anderes Kommunikationsmittel).

Nach Übergabe der Schlüsselwiederherstellungsanforderung können Sie den Status überprüfen, um festzustellen, ob die Anforderung genehmigt, zurückgewiesen oder noch anstehend ist.

Um eine Schlüsselwiederherstellungsanforderung auszugeben, gehen Sie wie folgt vor:

1. Rufen Sie die in Ihrem Unternehmen verwendete Website für den Zugriff auf die Webseite für die **Schlüsselwiederherstellungsanforderung** ab. Die URL hat das folgende Format:

   `http://`*`MyPublicWebServer`*`/`*`MyDomain`*`/KeyRecovery_Request.jsp`
2. Öffnen Sie Ihren Browser, und geben Sie die Website ein:
   - Wenn Sie Netscape verwenden, geben Sie die Website in das Textfenster bei **Adresse** ein.
   - Wenn Sie Internet Explorer verwenden, geben Sie sie ebenfalls bei **Adresse** in das Textfenster ein.
3. Drücken Sie die **Eingabetaste**.

   Die Webseite für die **Schlüsselwiederherstellungsanforderung** von Tivoli PKI wird angezeigt.
4. Wählen Sie unter **Zertifikatstyp** aus der Dropdown-Liste den Typ des Zertifikats aus, das wiederhergestellt werden soll.
5. Geben Sie unter **Vorname** Ihren Vornamen ein.
6. Geben Sie unter **Nachname** Ihren Nach- oder Familiennamen ein.
7. Geben Sie unter **Anforderungs-ID** die Anforderungs-ID ein (sofern bekannt), die beim ursprünglichen Zertifikatsregistrierungsprozess zugeordnet wurde. Ansonsten lassen Sie dieses Feld leer.
8. Klicken Sie auf **Schlüsselwiederherstellungsanforderung übergeben**.

9. Enthält die RA-Datenbank mehrere Einträge mit demselben Vor- und Nachnamen wie in Ihrer Schlüsselwiederherstellungsanforderung, wird eine Auswahlliste mit Schlüsselwiederherstellungsanforderungen angezeigt. Es handelt sich um eine Liste der Zertifikate bzw. Schlüssel, die Sie wiederherstellen können. Die Liste enthält den betreffenden registrierten Namen, die fortlaufende Zertifikatsnummer und die Datumsangaben für den Gültigkeitszeitraum.

   Wählen Sie das gewünschte Zertifikat bzw. den gewünschten Schlüssel aus, das bzw. der wiederhergestellt werden soll.

10. Klicken Sie auf **Schlüsselwiederherstellungsanforderung übergeben**.

11. Klicken Sie auf **Schlüsselwiederherstellungsstatus überprüfen**, um den Status Ihrer Anforderung festzustellen.

    Wenn der RA-Administrator die Anforderung genehmigt hat, wird die Seite **Schlüsselwiederherstellungsstatus – Status 'abgeschlossen'** angezeigt.

12. Klicken Sie auf **Wiederhergestellte PKCS #12-Datei sichern**, um die wiederhergestellte Datei downzuloaden und zu sichern.

4

Informationen zu...

Die folgenden Abschnitte definieren und beschreiben Konzepte, die mit Zertifikaten, der Registrierung, der Zertifizierung und dem Zugriff auf gesicherte Ressourcen im Zusammenhang stehen.

Registrierung

Registrierung bedeutet die Beantragung eines Zertifikats. Tivoli PKI bietet mehrere Registrierungsmethoden; die Regeln Ihres Unternehmens legen fest, welche Methoden; zur Verfügung stehen. Sie können über Ihren Web-Browser auf die Registrierungsformulare zugreifen, wenn Sie ein Zertifikat anfordern müssen. Auf der Registrierungs-Web-Seite können Sie eine Verbindung zu einem Registrierungsformular herstellen, dieses ausfüllen und anschließend übergeben. Sie können die folgenden Aktionen ausführen:

- Ein CA-Zertifikat anfordern, um sich auf Ihre Registrierungs-Tasks vorzubereiten.
- Ein Browser-Zertifikat für sich selbst anfordern.
- Ein Zertifikat für eine(n) bestimmte(n) Server oder Einheit anfordern.
- Sich selbst oder jemand anderen für ein Zertifikat vorab registrieren, das den Zugriff auf PKIX-kompatible Anwendungen ermöglicht.

Die Daten aus den Registrierungsformularen werden in Datenbanksätzen gespeichert, die von den Registratoren der Registrierungsstelle (RA) auf dem Desktop der Registrierungsstelle (RA Desktop) von Tivoli PKI angezeigt werden können.

Vorabregistrierung

Tivoli PKI ermöglicht es Programmen oder Administratoren, zukünftige Benutzer vorab zu registrieren.

Wenn Sie andere Personen für Zertifikate vorab registrieren wollen, befolgen Sie die Anweisungen des folgenden Szenarios:

- Sie benötigen Informationen zu der Person, die Sie vorab registrieren wollen. Entweder fragen Sie die betreffende Person selbst, oder Sie ziehen Aufzeichnungen des Unternehmens heran wie beispielsweise Informationen aus einer Datenbank.
- Sie greifen über Ihren Web-Browser auf die Registrierungsseite zu. Es gibt ein eigenes Registrierungsformular für die Vorabregistrierung.
- Sie füllen das Formular mit den Informationen aus, die jeweils auf die Person und den Zertifikatstyp zutreffen. Anschließend übergeben Sie das Formular.
- Sie überprüfen den Status der Anforderung.

Wenn der Antrag für die Vorabregistrierung genehmigt ist, erhalten Sie eine Transaktions-ID, ein Kennwort und die Website der RA, die die Genehmigung der Anforderung durchgeführt hat.

- Diese Informationen teilen Sie der vorab registrierten Person mit — per Telefon, E-Mail oder persönlich. Um es für die betreffende Person besonders einfach zu machen, haben Sie auch die Möglichkeit, ihr eine Vorabregistrierungsdatei zur Verfügung zu stellen, in der weitere Anforderungsinformationen enthalten sind. Wenn die Person bereit ist, ihr Zertifikat anzufordern, verwendet sie die von Ihnen gelieferten Informationen.

Webbrowserunterstützung

Mit Tivoli PKI können Sie eine Registrierungsanforderung erstellen, indem Sie ein Registrierungsformular ausfüllen und über einen der beiden folgenden Web-Browser übergeben:

- Microsoft Internet Explorer, ab Release 5.0.
- Netscape Navigator oder Netscape Communicator, Version 4.7*x*.

Registrierung

Die Registrierung ist der Prozess, über den ein digitales Zertifikat genehmigt und an eine Person oder andere Entität ausgestellt wird. Bei Tivoli PKI wertet ein Programm oder ein Registrator vor der Registrierung die Informationen aus, die zusammen mit der Registrierungsanforderung zur Verfügung gestellt wurden. Unabhängig davon, ob die Anforderung genehmigt wird oder nicht, erstellt die Tivoli PKI-Registrierungsstelle (RA) in der Registrierungsdatenbank einen Datensatz für die entsprechende Anforderung. Wenn entschieden wird, das Zertifikat zu genehmigen, wird es vom Tivoli PKI-Zertifikatsaussteller (CA) ausgestellt.

Unternehmensregel

Wenn ein Programm oder ein Registrator Ihre Angaben zur Registrierung auswertet, werden auf einige dieser Registrierungsinformationen zur Registrierung die Regeln Ihres Unternehmens angewandt. Die Art der Informationen, die ein Programm auswerten kann, ist weniger komplex als die Informationen, die von einem Registrator ausgewertet werden können. Es handelt sich normalerweise um präzise Werte wie beispielsweise die Mindestanzahl der an einem Wohnort verbrachten Jahre. Mit Tivoli PKI kann Ihr Unternehmen einem solchen Programm die entsprechenden Informationen zu den Unternehmensregeln zur Verfügung stellen. Das Programm verwendet diese Informationen dann bei der Auswertung.

Registrierungsstellen

Bei Tivoli PKI handelt es sich bei den RAs um eine Server-Anwendung. Sie führt einige der Verwaltungs-Tasks aus, die für die Registrierung von Benutzern erforderlich sind. Dazu gehört unter anderem folgendes:

- Die Identität eines Benutzers bestätigen.
- Überprüfen, ob der Absender der Anforderung Anspruch auf ein Zertifikat mit den angeforderten Attributen und Berechtigungen hat.
- Anforderungen genehmigen oder zurückweisen, um Zertifikate zu erstellen bzw. zu widerrufen.
- Zertifikate aussetzen oder reaktivieren
- Überprüfen, ob eine Person, die versucht, auf eine gesicherte Anwendung zuzugreifen, über den privaten Schlüssel verfügt, der dem öffentlichen Schlüssel im Zertifikat zugeordnet ist.

Registrierungsdatenbanken

Eine Tivoli PKI-Registrierungsdatenbank speichert Registrierungssätze. Bei der Registrierungsdatenbank handelt es sich um eine relationale Datenbank, die mit IBM DB2 Universal Database erstellt wurde. Die Sätze werden von Tivoli PKI verschlüsselt. Über den RA Desktop kann ein autorisierter Registrator jedoch die meisten der Registrierungsinformationen lesen.

Registrierungsdomänen

Jedes Tivoli PKI-System verfügt über eine eigene Registrierungsdomäne. Diese Domäne definiert die Unternehmensregeln, Zertifikatsregeln und Ressourcen, die mit der Registrierung und Zertifizierung in Ihrem Unternehme in Zusammenhang stehen. Benutzer, die auf eine Ressource zugreifen wollen, müssen für die Domäne dieser Ressource registriert sein.

Wenn die RA-Server-Software installiert ist, enthält sie das Gerüst, mit dem ein Unternehmen eine Registrierungsfunktion aufbauen kann. Sie kann alle Sprachen und Regeln verwenden, die von der Registrierungsstelle (RA) unterstützt werden. Der Domänenname, die Sprache und der Installationspfad bilden die Website für den Zugriff auf ein bestimmtes Exemplar der Registrierungsfunktion.

Beispiel: Wenn der Name Ihres öffentlichen Webservers 'Mein_öffentlicher_Web-Server' (MyPublicWebServer) und der Name Ihrer Registrierungsdomäne 'Meine_Domäne' (MyDomain) lautet, würden Sie für den Zugriff auf die Registrierungsfunktion die folgende Website verwenden:

```
http://MyPublicWebServer/MyDomain/index.jsp
```

Ein Tivoli PKI-System enthält eine standardmäßige Java-Server-Seite (index.jsp) mit der entsprechenden Registrierungsfunktion. Diese Seite wird auf der Registrierungswebsite Ihrer Registrierungsdomäne angezeigt. Sie stellt die folgenden Registrierungsservices zur Verfügung:

- Potenzielle Benutzer rufen diese Web-Seite auf, um ein Zertifikat anzufordern und um ihre eigenen Browser-Zertifikate zu erneuern oder zu widerrufen.
- Administratoren können die Registrierungs-Web-Seite auch dazu aufrufen, um andere Benutzer vorab zu registrieren.

Tivoli PKI-Registratoren greifen auf den RA Desktop zu, um mit den Registrierungsanforderungen und Zertifikaten zu arbeiten, die einer Registrierungsdomäne zugeordnet sind.

Registrierungssätze

Jede Anforderung für ein Zertifikat ist ein Registrierungsformular, das an die Tivoli PKI-RA übergeben wird. Jede Registrierungsanforderung führt zu einem Satz in der Registrierungsdatenbank. Aktualisierungen an diesem Satz spiegeln jede für die Anforderung ausgeführte Aktion wider, selbst eine Zurückweisung der Anforderung. Wenn ein Zertifikat erstellt wird, spiegelt derselbe Satz alle Ereignisse wider, die mit diesem Zertifikat in Zusammenhang stehen. Demnach enthält der Registrierungssatz alle Ereignisse im Verarbeitungszyklus der Anforderung und des zugeordneten Zertifikats.

Satzattribute

Die Attribute eines Satzes in der Registrierungsdatenbank sind Variablen, die die Registrierungsanforderung beschreiben. Bei ausgeführten Anforderungen beschreiben die Variablen auch das genehmigte Zertifikat. Andere Attribute sind Verarbeitungsvariablen, die Ihrem Unternehmen dabei helfen, ihre Unternehmensregeln umzusetzen. Viele Attribute und ihre zugehörigen Werte können von den Registratoren über den RA Desktop angezeigt werden.

Zertifizierung

Zertifizierung bedeutet die Erstellung eines digitalen Zertifikats für eine Entität oder eine Person. Bei Tivoli PKI erfolgt die Zertifizierung erst nach der Überprüfung und Genehmigung einer Registrierungsanforderung. Infolge der Registrierung stellt der Zertifikatsaussteller (CA) die Zertifikate aus. Bei Tivoli PKI stimmt der ausgestellte Zertifikatstyp mit den Regeln Ihres Unternehmens überein.

Zertifikatsaussteller

Bei Tivoli PKI ist der Zertifikatsaussteller (CA) ein Server-Programm, das für das Ausstellen digitaler Zertifikate verantwortlich ist, die mit den Regeln Ihres Unternehmens übereinstimmen.

Tivoli PKI unterstützt die gegenseitige Zertifizierung, bei der CAs, die sich gegenseitig vertrauen, die Zertifikate des jeweils anderen CA als Authentizitätsnachweis akzeptieren. Tivoli PKI unterstützt ebenfalls eine CA-Hierarchie. CAs vertrauen den CAs, die in der Hierarchie über ihnen stehen, und akzeptieren die Zertifikate dieser CAs als Authentizitätsnachweise.

Zertifikatswiderrufslisten (CRL)

Die Tivoli PKI-RA veröffentlicht in regelmäßigen Abständen eine Zertifikatswiderrufsliste (CRL). Sie enthält die Zertifikate, die nicht mehr gültig sind, damit Inhaber solcher Zertifikate, die diese vorlegen, nicht authentifiziert werden.

Alle CAs, RAs und Anwendungen können auf diese Liste zugreifen, um festzustellen, ob ein Zertifikat widerrufen wurde oder nicht. Dies ist eine Maßnahme, mit der die Tivoli PKI-RA für Sicherheit sorgt, wenn Benutzer versuchen, auf die gesicherten Anwendungen Ihres Unternehmens zuzugreifen.

Verzeichnisse (Directory)

Das Verzeichnis, das von Tivoli PKI zum Speichern von Zertifikaten verwendet wird, ist das IBM Directory. Dieses Directory kann ein Verzeichnis sein, das Ihr Unternehmen speziell zur Verwendung mit Tivoli PKI definiert hat. Es kann sich auch um ein Verzeichnis handeln, das Sie zuvor installiert haben und mit anderen Anwendungen verwenden.

Für den Zugriff auf das Directory verwendet Tivoli PKI das Lightweight Direct Access Protocol (LDAP), ein Direktzugriffsprotokoll mit reduziertem Funktionsumfang.

Registrierte Namen

Der registrierte Name (DN, Distinguished Name) ist ein Element des Directory-Eintrags für ein digitales Zertifikat. Er identifiziert eindeutig die Position eines Eintrags in der hierarchischen Struktur des Directory.

Zertifikate

Ein Zertifikat ist ein digitaler Identitätsnachweis, der von einem CA unterzeichnet ist, der für die Identität des Zertifikatsinhabers garantiert. Der Inhaber kann das Zertifikat zur Authentifizierung verwenden, wenn er mit anderen kommuniziert oder wenn er den Zugriff auf eine gesicherte Anwendung anfordert. Bei Tivoli PKI müssen selbst Server, Anwendungen und Einheiten wie Drucker und Smart Cards über Zertifikate verfügen, um sich gegenüber von Benutzern und gegenseitig zu authentifizieren.

Tivoli PKI unterstützt X.509v3-Zertifikate in den folgenden Kategorien:

- Browser-Zertifikate
- Server-Zertifikate
- Einheitenzertifikate
- Zertifikate für den Zugriff auf PKIX-kompatible Anwendungen
- Gegenseitig ausgestellte Zertifikate für CAs

Tivoli PKI unterstützt außerdem die folgenden Protokolle:

- SSL
- S/MIME
- IPSec
- PKIX CMP

Eine standardmäßige Tivoli PKI-Installation stellt eine Reihe von verschiedenen Zertifikatstypen zur Verfügung, die auf diesen Kategorien und Protokollen basieren. Registrierte Benutzer können ihrem Bedarf entsprechende Zertifikate anfordern. Im Abschnitt „Gelieferte Zertifikatstypen” auf Seite 28 werden die Zertifikatstypen beschrieben.

Browserzertifikate

Ein Browser-Zertifikat ist ein digitaler Identitätsnachweis, der normalerweise in einer verschlüsselten Datei von Ihrem Web-Browser gespeichert wird. Bestimmte Anwendungen erlauben die Speicherung der Schlüssel auf einer Smartcard oder einem anderen Datenträger. In einem Tivoli PKI-System können Sie ein Browser-Zertifikat direkt über Ihren Web-Browser anfordern. Später können Sie bei Bedarf auf die Webseite für die Registrierung zurückkehren und das Zertifikat erneuern oder widerrufen.

CA-Zertifikate

Alle Browser, Server, Einheiten und Anwendungen, die über ein Zertifikat zur Vorlage bei Tivoli PKI-Servern verfügen, müssen ebenfalls ein kompatibles CA-Zertifikat besitzen. Dieses Zertifikat ist erforderlich, um die Datenfernverarbeitung von Servern zu authentifizieren, die im Besitz von Zertifikaten sind, die vom Tivoli PKI-CA ausgestellt sind.

Ihr Browser muss über ein Tivoli PKI-CA-Zertifikat verfügen, damit Sie die gesicherten Tivoli PKI-Registrierungsservices verwenden können. Sie können dieses Zertifikat abrufen, wenn Sie die Web-Seiten von Tivoli PKI zur Registrierung das erste Mal besuchen. Wann immer Sie danach ein Zertifikat von den Registrierungsservices anfordern, können Sie ein entsprechendes CA-Zertifikat herunterladen, das mit dem angeforderten Zertifikat kompatibel ist.

Beispiel: Wenn Sie ein zweijähriges SSL-Browser-Zertifikat anfordern, können Sie ein CA-Zertifikat herunterladen, das mit diesem Zertifikat kompatibel ist.

Anmerkung: Frühere Releases von Netscape konnten ein Site-Zertifikat akzeptieren, das von einem Tivoli PKI-Server vorgelegt wurde. Dieses Zertifikat war für Kommunikationen mit dem Server akzeptabel, die entweder von der Server-Seite oder von der Client-Seite authentifiziert wurden. Das neueste Release von Netscape erfordert für Sitzungen, die von der Client-Seite authentifiziert wurden, nun jedoch ein CA-Zertifikat.

Server- oder Einheitenzertifikate

Wenn dies im Rahmen Ihrer Tätigkeit erforderlich ist, können Sie ein Zertifikat für einen Server oder eine Einheit anfordern. Verwenden Sie dazu das Registrierungsformular, das über Ihren Web-Browser zur Verfügung gestellt wird.

Der Server oder die Einheit, für den bzw. die Sie ein Zertifikat anfordern, muss das Anforderungsformat PKCS #10 verwenden.

Zertifikatserweiterungen

Zertifikatserweiterungen sind wahlfreie Elemente im Format eines X.509v3-Zertifikats. Die Erweiterungen ermöglichen es, dem Zertifikat weitere Felder hinzuzufügen. Tivoli PKI stellt eine Gruppe von Zertifikatserweiterungen zur Verfügung, um Ihr Unternehmen in die Lage zu versetzen, die von ihm ausgestellten Zertifikate anzupassen. Diese zusätzlichen Felder werden *Geschäftsprozessvariablen* genannt.

Gültigkeitsdauer von Zertifikaten

Wenn Sie ein Zertifikat anfordern, leiten Sie einen Verarbeitungszyklus ein, der sich über die gesamte Laufzeit dieses Identitätsnachweises erstreckt. Dieser Verarbeitungszyklus endet, wenn das Zertifikat widerrufen wird oder abläuft.

Wenn ein Zertifikat erneuert wird, wird ein neuer Datensatz in der Registrierungsdatenbank erstellt.

Erneuerbarkeit

Die Erneuerbarkeit ist eine der Eigenschaften eines Zertifikats, die der Registrator für Sie über den RA Desktop ändern kann:

- Wenn Ihr Zertifikat erneuerbar ist, können Sie ein neues Zertifikat beantragen, während das alte noch gültig ist. Der Besitz eines erneuerbaren Zertifikats vereinfacht den Registrierungsprozess und verringert den Registrierungsaufwand.

  Wenn Sie über ein erneuerbares Browser-Zertifikat verfügen, können Sie dessen Erneuerung auf der Registrierungs-Web-Seite anfordern.

- Wenn Ihr Zertifikat nicht erneuerbar ist, müssen Sie warten, bis es abläuft, und sich dann erneut registrieren, falls Sie weiterhin ein Zertifikat benötigen. Wenn Sie sich registrieren, müssen Sie alle Informationen zur Verfügung stellen, die Sie auch bei der ersten Registrierung angegeben haben.

Zugriff auf gesicherte Ressourcen

Dieser Abschnitt erläutert die Verwendung und Verwaltung von Zertifikaten.

Zugriffssteuerung

Eine Zugriffssteuerungsliste (ACL, Acces Control List) authentifiziert und genehmigt interne Tivoli PKI-Benutzer, -Einheiten und -Software. Beispiel: Das RA Desktop-Unterstützungs-Servlet verwendet die ACL, um Registratoren zu authentifizieren und zu genehmigen, bevor diese auf den RA Desktop zugreifen können.

Authentifizierung und Berechtigung

Bei der Authentifizierung wird eine Identität überprüft, während eine Genehmigung die Berechtigung für eine Aktion ist. Tivoli PKI ermöglicht es Ihrem Unternehmen, sowohl eine Authentifizierung als auch eine Genehmigung zu verlangen, bevor Benutzer auf gesicherte Anwendungen zugreifen können. Im Gegenzug können Zertifikatsinhaber darauf vertrauen, dass die von ihnen genutzten Anwendungen auch sicher sind.

Digitale Unterschriften

Mit Hilfe eines Ihrer Zertifikate können Sie eine Datei mit einer digitalen Unterschrift versehen. Diese Unterschrift sagt dem Empfänger einer Datei beim Öffnen, ob deren Inhalt seit der Unterzeichnung geändert worden ist. Mit der digitalen Unterschrift wird der Inhalt der Datei nicht verschlüsselt.

Sicherung und Wiederherstellung von Schlüsseln

Tivoli PKI stellt eine Funktion zum Anfordern von Schlüsselsicherungen und -wiederherstellungen zur Verfügung. Diese Funktion ermöglicht das Sichern und Wiederherstellen von Endentitätszertifikaten und zugehörigen privaten Schlüsseln, die von Tivoli PKI zertifiziert wurden.

Mit Hilfe dieser Funktion können verlorene, vergessene oder anderweitig abhanden gekommene Zertifikate und private Schlüssel wiederhergestellt werden. Betrachten Sie folgendes Szenario als Beispiel: Ein Angestellter führt routinemäßig eine Sicherung seiner Zertifikate und privaten Schlüssel aus und scheidet dann plötzlich aus der Firma aus, ohne alle privaten Schlüssel zurückzugeben, die für den Zugriff auf diese Informationen erforderlich sind. Durch Ausgabe einer Wiederherstellungsanforderung können Sie Informationen abrufen, die vormals verloren gewesen wären.

Im Allgemeinen umfasst der Sicherungsprozess die Erstellung einer PKCS #12-Datei durch den Benutzer. Diese Datei enthält das Zertifikat und den privaten Schlüssel des betreffenden Benutzers. Der Benutzer gibt über einen unterstützten Browser eine Sicherungsanforderung aus und verwendet dabei die PKCS #12-Datei als Eingabe. Die Datenbank ’krbdb’ für die Wiederherstellung von Schlüsseln wird aktualisiert und enthält die entsprechenden Zugriffsinformationen. Die Wiederherstellung von Schlüsseln funktioniert auf ähnliche Weise: Zunächst wird eine Wiederherstellungsanforderung für die zuvor gesicherte PKCS #12-Datei ausgegeben. Nachdem die Anforderung vom RA-Administrator genehmigt wurde, wird die Datei zum Downloaden für Sie bereitgestellt.

5

Referenzinformationen

Die folgenden Abschnitte enthalten Feldbeschreibungen, zulässige Feldwerte und die Bedeutung der Zertifikatsattribute. Ebenso enthalten sind Informationen, die Ihnen bei der Verwendung von Tivoli PKI in einer anderen Sprache als Englisch helfen können.

Registrierungsformular auf der Webseite

Das Registrierungsformular enthält Abschnitte für Daten über den potenziellen Zertifikatsinhaber und für Daten über die Anforderung des Zertifikats. Einige Felder in diesen Abschnitten stehen nur für bestimmte Registrierungstypen zur Verfügung.

Anmerkung: Wenn Ihr Unternehmen die Registrierungsformulare anpasst, kann deren Inhalt von der Beschreibung in diesem Handbuch abweichen.

Die **Registrierungsinformationen** enthalten die folgenden Felder, sofern sie auf den angeforderten Zertifikatstyp zutreffen:

Zertifikatstyp
Wählen Sie einen Wert aus der Liste aus. Im Abschnitt „Gelieferte Zertifikatstypen" auf Seite 28 werden die Zertifikatstypen beschrieben, die mit einer Standardinstallation zur Verfügung gestellt werden.

Vorname
Geben Sie in dieses Feld Ihren Vornamen ein. Die Angabe eines zweiten Vornamens oder dessen Anfangsbuchstabens steht Ihnen frei.

Bei einer Vorabregistrierung beziehen sich diese Angaben auf die Person, die Sie vorab registrieren.

Nachname
Geben Sie in dieses Feld Ihren Nachnamen oder Familiennamen ein.

Bei einer Vorabregistrierung beziehen sich diese Angaben auf die Person, die Sie vorab registrieren.

E-Mail-Adresse
Geben Sie in dieses Feld Ihre E-Mail-Adresse ein, einschließlich des kommerziellen A (@) und aller Punkte (.). Für einige Zertifikatstypen (beispielsweise Zertifikate für sichere E-Mails) ist diese Adresse erforderlich. Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie eine E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie diese Option aus, um per E-Mail vom Ergebnis der vorliegenden Registrierungsanforderung benachrichtigt zu werden.

Anmerkung: Wenn der RA-Server auf einer Windows NT-Plattform in Ihrem Unternehmen installiert ist, muss die Konfigurationsdatei (raconfig.cfg) der Registrierungsfunktion möglicherweise aktualisiert werden, damit sie auf einen SMTP-Host verweist, um diese Funktion zu aktivieren. Das Handbuch *Tivoli PKI Anpassung* enthält weitere Informationen hierzu.

Identifikationsprüfungsfrage
Dies ist eine Frage, deren Antwort nur Sie kennen und die verwendet werden kann, um Ihre Identität zu überprüfen bzw. um zu verhindern, dass sich jemand anderes für Sie ausgibt. Wenn Sie den Status der Registrierungsanforderung überprüfen, wird Ihnen diese Frage gestellt. Sie müssen die Identifikationsprüfungsfrage beantworten, unabhängig davon, ob die Anforderung für Sie selbst, für einen Server oder eine Einheit oder zur Vorabregistrierung einer anderen Person gestellt wird.

Identifikationsprüfungsantwort
Dies ist die Antwort auf die Identifikationsprüfungsfrage, die Sie angegeben haben. Geben Sie eine Antwort ein, die leicht zu merken ist. Wenn Sie den Status Ihrer Anforderung überprüfen, müssen Sie genau dieselbe Antwort eingeben.

Anmerkung: Bei der Antwort ist die Groß-/Kleinschreibung zu beachten.

Kennwort
(*Nur Vorabregistrierung*) Dies ist das Kennwort, das die von Ihnen vorab registrierte Person der Client-Anwendung zur Verfügung stellen muss, wenn sie bereit ist, das Zertifikat herunterzuladen. Verwenden Sie die Zeichen A-Z, a-z und 0–9. Das Kennwort darf zwischen 8 und 32 Zeichen enthalten.

Wenn Sie kein Kennwort angeben, generiert die Registrierungsfunktion für Sie ein Kennwort, das 10 Zeichen enthält. Bei Genehmigung der Vorabregistrierungsanforderung erhalten Sie dieses Kennwort zusammen mit einer Transaktions-ID.

Kennwort bestätigen
(*Nur Vorabregistrierung*) Geben Sie dasselbe Kennwort nochmals ein.

Die **Zertifikatsanforderungsinformationen** enthalten die folgenden Felder:

PKCS #10-Zertifikatsanforderung
(*Nur Server- oder Einheitenregistrierung*) Dieses Feld ist für den Inhalt der PKCS #10-Zertifikatsanforderung, die von dem Server bzw. der Einheit generiert wurde, für den bzw. die Sie ein Zertifikat anfordern. Wenn die Anforderung in einer Datei gespeichert wurde, öffnen Sie die Datei mit einem Texteditor wie beispielsweise Windows Notepad. Kopieren Sie den Inhalt, und fügen Sie ihn in das Textfenster des Registrierungsformulars ein.

Allgemeiner Name
Dies ist ein Name zur Identifizierung dieses Zertifikats.

- Bei Personen ist dies normalerweise der vollständige Name der betreffenden Person.
- Bei Servern oder Einheiten ist dies gewöhnlich der Host-Name. Sie müssen diesen Wert eingeben, wenn im Feld für die PKCS #10-Zertifikatsanforderung kein Host-Name vorhanden ist.

Schlüsselgröße

(*Nur Netscape-Browser-Registrierung*) Dies ist die Schlüsselgröße für das Schlüsselpaar aus öffentlichem und privatem Schlüssel. Wählen Sie einen Wert aus. Größere Schlüssel sind sicherer, verlängern jedoch auch die Zeit, die erforderlich ist, um eine Verbindung zu einer sicheren Sitzung herzustellen.

Verschlüsselungsserviceanbieter

(*Nur Internet Explorer-Browser-Registrierung*) Dies ist der Verschlüsselungsserviceanbieter (Cryptographic Service Provider, CSP), der Ihr Schlüsselpaar aus öffentlichem und privatem Schlüssel generieren soll. Wählen Sie einen Wert aus. Größere Schlüssel sind sicherer, verlängern jedoch auch die Zeit, die erforderlich ist, um eine Verbindung zu einer sicheren Sitzung herzustellen.

Die Standardeinstellung ist Microsoft Base Cryptographic Provider. Dieser Verschlüsselungsserviceanbieter stellt Schlüssel mit 512 Bit für die Verschlüsselung zur Verfügung.

Microsoft Enhanced Cryptographic Provider (sofern auf Ihrem System installiert) stellt Schlüssel mit 1024 Bit zur Verfügung.

Schlüsselsatz

(*Nur Internet Explorer-Browser-Registrierung*) Dies ist das zu verwendende Schlüsselpaar. Wählen Sie **Neuen Schlüsselsatz generieren** aus, oder öffnen Sie die Liste, und wählen Sie eines der vorhandenen Schlüsselpaare aus.

Name des neue Schlüsselsatzes

(*Nur Internet Explorer-Browser-Registrierung*) Dies ist der Name des neuen Schlüsselsatzes, der generiert werden soll. Sie können dieses Feld auch leer lassen und eine GUID (Globally Unique Identifier) für den Namen generieren lassen. In diesem Fall ist es jedoch schwieriger, das Schlüsselpaar wiederzuerkennen.

Zusätzliche Sicherheitsoptionen

Dies sind zusätzliche Sicherheitsfunktionen, die Microsoft Internet Explorer für Ihr neues Schlüsselpaar zur Verfügung stellt. Wenn Sie diese Option auswählen, zeigt ihr Web-Browser unmittelbar nach Übergabe dieses Registrierungsformulars entsprechende Internet Explorer-Dialoge an, mit denen Sie diese Optionen einstellen können.

Firmenname

Dies ist der gesetzlich registrierte Name Ihrer Firma.

Abteilung

Dies ist der Name Ihrer Abteilung, beispielsweise Personalabteilung oder Softwareentwicklung.

Adresse

Dies ist die Adresse (Straße, Hausnummer) Ihres Unternehmens.

Ort Dies ist die Stadt, in der Ihr Unternehmen ansässig ist, beispielsweise Chicago oder Berlin.

Bundesland

Dies ist das Bundesland, in dem Ihr Unternehmen ansässig ist. Ob Sie den vollständigen Namen des Bundeslandes schreiben oder eine offizielle Abkürzung verwenden, hängt von Ihren Registrierungsregeln ab.

Land Dies ist das Land, in dem Ihr Unternehmen ansässig ist. Wählen Sie einen Wert aus.

Domänenname
Der Host-Name der Maschine, auf der ein Zertifikat installiert wird. Für Serverzertifikate und Endbenutzerzertifikate (Browserzertifikate und Zertifikate, die über die Vorabregistrierung abgerufen werden) ist dieses Feld wahlfrei. Wenn Sie dieses Feld integrieren wollen, müssen Sie die Maschine identifizieren, auf der der Browser oder der Webserver installiert ist. Für IPSec-Zertifikate müssen Sie die IPSec-Einheit identifizieren, auf der das Zertifikat installiert wird.

Gelieferte Zertifikatstypen

Ein Tivoli PKI-System stellt mehrere Zertifikatstypen für die unterstützten Zertifikatskategorien und -protokolle zur Verfügung. Zu den Abwandlungen gehören verschiedene Gültigkeitszeiträume. Der Name des Zertifikats zeigt an, wie lange es gültig ist und wofür der Schlüssel hauptsächlich verwendet wird. Das Glossar enthält eine Beschreibung der jeweiligen Funktionen.

Gegenseitig ausgestelltes CA-Zertifikat
Mit diesem Zertifikat kann der Zertifikatsaussteller (CA), dem dieses Zertifikat gehört, seine Zertifikate vom ausstellenden CA genehmigen lassen. Das Zertifikat stellt die Funktionen für digitale Unterschriften und Unbestreitbarkeit zur Verfügung.

Datenverschlüsselungszertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber Daten verschlüsseln. Das Zertifikat ist nicht für andere Zwecke gedacht.

E-Mail-Schutzzertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber das S/MIME-Protokoll (Secure Multi-Purpose Internet Mail Exchange) verwenden. Dieses Protokoll schützt E-Mail und andere MIME-Objekte. Es stellt die Funktionen für die Authentifizierung des Absenders, Nachrichtenintegrität, Unbestreitbarkeit des Absenders und Vertraulichkeit zur Verfügung. Es wird normalerweise von Endbenutzer gewählt.

IPSec-Zertifikat - 1 Jahr und 2 Jahre
Dieses Zertifikat gewährleistet die Integrität und Vertraulichkeit von Daten, die in IP-Paketen (IP = Internet Protocol) über das Internet gesendet werden. IPSec-Zertifikate sind eher für Daten als für Benutzer gedacht. Sie sind häufig einem Router zugeordnet.

Zertifikat für Schlüsselcodierung (ausschließlich) - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber Schlüssel codieren. Das Zertifikat ist nicht für andere Zwecke gedacht.

Unbestreitbarkeitszertifikat - 1 Jahr und 2 Jahre
Dieses Zertifikat stellt die Funktionen für Nachrichtenverschlüsselung und digitale Unterschriften zur Verfügung, um die Unbestreitbarkeit des Nachrichtenabsenders bzw. die Unbestreitbarkeit der Nachrichtenzustellung zu gewährleisten.

Zertifikat für Unterschrift (ausschließlich) - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber Dateien digital unterzeichnen. Das Zertifikat ist nicht für andere Zwecke gedacht.

Web-Client-Authentifizierungszertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann ein Web-Browser an einer vom Client authentifizierten SSL-Sitzung teilnehmen. Der Benutzer des Browsers kann mit diesem Zertifikat auf eine spezifische gesicherte Web-Site zugreifen. Das Zertifikat stellt die Funktionen für digitale Unterschriften, Unbestreitbarkeit und Schlüsselcodierung zur Verfügung. Es wird normalerweise von Endbenutzer gewählt.

Web-Server-Authentifizierungszertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann ein Server an einer vom Server authentifizierten SSL-Sitzung teilnehmen. Das Zertifikat stellt die Funktionen für digitale Unterschriften und Schlüsselcodierung zur Verfügung.

Registrierte Personen oder Personen, die jemand anderen vorab registrieren, können einen geeigneten Zertifikatstyp anfordern. Die verfügbaren Zertifikatstypen werden in den Registrierungsformularen im Feld **Zertifikatstyp** aufgelistet.

Anmerkung: Die angezeigte Liste entspricht unter Umständen nicht der Liste in diesem Handbuch. Es kann sein, dass Ihr Unternehmen die Namen oder sogar die verfügbaren Zertifikatstypen geändert hat.

Gründe für das Widerrufen eines Zertifikats

Wenn Sie ein Zertifikat widerrufen, müssen Sie dafür eine Begründung auswählen. Die folgenden Begründungen sind zulässig und können ausgewählt werden:

Der CA-Schlüssel war beschädigt
Der Schlüssel des Zertifikatsausstellers (CA), der das Zertifikat ausgestellt hat, wurde beschädigt.

Das Zertifikat wurde ersetzt
Sie haben ein neues Zertifikat und benötigen das vorliegende nicht mehr.

Keine Begründung
Sie geben keine Begründung an.

Der ursprüngliche Verwendungszweck des Zertifikats ist nicht mehr gültig
Sie benötigen das Zertifikat nicht mehr für dessen ursprünglichen Verwendungszweck. Beispiel: Sie müssen nicht mehr auf die Ressource oder die Anwendung zugreifen, für die das Zertifikat ausgestellt wurde.

Benutzer hat Zugehörigkeit geändert
Sie arbeiten nicht mehr mit dem Unternehmen zusammen, für das das Zertifikat gilt.

Der Benutzerschlüssel war beschädigt
Ihr privater Schlüssel wurde beschädigt.

Anmerkung: Auf den Registrierungsformularen werden die zulässigen Begründungen im Feld **Begründung** aufgelistet, wenn Sie ein Zertifikat auf der Registrierungs-Web-Seite widerrufen.

Systemvoraussetzungen für die Browserregistrierung

Für die Verwendung der Browser-Registrierungsformulare mit der Registrierungsfunktion empfiehlt IBM die folgende Datenstationskonfiguration.

- Konfiguration der physischen Maschine:
  - Intel 486-Prozessor mit 166 MHz und 32 MB RAM als Mindestanforderung (Vorzugsweise Intel -Pentium-Prozessor mit 200 MHz und mindestens 64 MB RAM)
  - Computer-Bildschirm, der mindestens VGA-Auflösung unterstützt
- Eines der folgenden Betriebssysteme:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT
- Einen der folgenden Web-Browser:
  - Netscape Navigator oder Netscape Communicator, Version 4.7*x*
  - Microsoft Internet Explorer, Version 5.0 oder höher
- Wahlfrei: Unterstützung für eine physische Smart Card. Wenn Sie planen, Zertifikate auf Smart Cards zu speichern, müssen Sie Ihren Browser möglicherweise mit einer für die entsprechende Smart Card erforderlichen Version aktualisieren. Beispiel: IBM Smart Card Security Kit erfordert einen der folgenden Browser:
  - Netscape Navigator oder Netscape Communicator, Version 4.7*x*
  - Microsoft Internet Explorer, Version 5.0 oder höher

Informationen zur Unterstützung in der Landessprache

In diesem Abschnitt werden die Unterschiede zusammengefasst, die zwischen der englischen Version von Tivoli PKI und den Versionen in anderen unterstützten Sprachen bestehen. Wenn Sie Zertifikate anfordern oder verwalten, die eine nicht-englische Tivoli PKI-Version verwenden, lesen Sie diesen Abschnitt, um zu erfahren, welche Unterschiede es beim Anzeigen und Verarbeiten von Daten in Ihrer jeweiligen Sprache möglicherweise gibt.

Es folgt eine Liste der Sprachencodes für die unterstützten Sprachen:

- `de_DE` für Deutsch
- `en_US` für Englisch
- `es_ES` für Spanisch
- `fr_FR` für Französisch
- `it_IT` für Italienisch
- `ja_JP` für Japanisch
- `ko_KR` für Koreanisch
- `pt_BR` für brasilianisches Portugiesisch
- `zh_CN` für vereinfachtes Chinesisch
- `zh_TW` für traditionelles Chinesisch

Zertifikate mit Nicht-ASCII-DNs anfordern

Sie können Tivoli PKI dazu verwenden, Zertifikate mit Nicht-ASCII-DNs (Distinguished Names = registrierte Namen) anzufordern, wie beispielsweise Zertifikate, in denen für den allgemeinen Namen Zeichen in der für die jeweilige Landessprache spezifischen Schreibweise verwendet werden. Die DNs der von Tivoli PKI erstellten Zertifikate werden in druckbaren Zeichen, Teletex (T.61)- oder UTF-8-Zeichen codiert. Normalerweise werden DNs, die Zeichen in der für europäische Landessprachen spezifischen Schreibweise enthalten, in Teletex codiert und DNs, die Zeichen in der für Chinesisch, Japanisch oder Koreanisch spezifischen Schreibweise enthalten, in UTF-8. Je nach Browser-Typ und dessen jeweiliger Lokalisierung für Ihre Umgebung werden diese Zertifikate möglicherweise nicht korrekt angezeigt.

Netscape für Zertifikate mit Nicht-ASCII-DNs verwenden

Netscape-Browser können Zertifikate, die mit UTF-8 codiert sind, nicht verarbeiten. Tivoli PKI codiert DNs, die Doppelbytezeichen enthalten (in Chinesisch, Japanisch oder Koreanisch) mit UTF-8. Da die derzeit verfügbaren Versionen von Netscape die mit UTF-8 codierten Zertifikate nicht verarbeiten können, kann Netscape nicht zum Anforderung oder Importieren von Zertifikaten verwendet werden, deren DNs Zeichen in chinesischer, japanischer oder koreanischer Landesspreche enthalten. Verwenden Sie stattdessen Microsoft Internet Explorer zum Anfordern von Zertifikaten in diesen Landessprachen.

Netscape zum Anzeigen der Schlüsselgröße verwenden

Bei der Verwendung von Netscape mit einer nicht-englischen Version des Browser-Registrierungsformulars wird unleserlicher Text im Feld für die Schlüsselgröße in Kästchen ([][][]) angezeigt. Dieser Text wird intern vom Browser generiert und weist kein UTF-8-Format auf. Der Netscape-Browser generiert diese Textzeichenfolge ausschließlich in den Basiszeichensätzen (wie beispielsweise ISO-8859-1 für Englisch und westeuropäische Landessprachen, Big5 für traditionelles Chinesisch und BG2312 für vereinfachtes Chinesisch).

Da die JSP-Registrierungsseiten in UTF-8 codiert sind, erkennt der Browser die Zeichenfolge im Basiszeichensatz nicht. Daher kann diese Zeichenfolge im Browser nicht mit dem UTF-8-Zeichensatz angezeigt werden.

Die Auswahlmöglichkeiten für die Schlüsselgröße in einer US-Version des Netscape-Browsers lauten wie folgt:

- 1024 (High Grade)
- 768 (Medium Grade)
- 512 (Low Grade)

Aufgrund von Exporteinschränkungen durch die US-Regierung enthält die Liste für eine nicht-englische Version des Browsers wahrscheinlich nur einen Eintrag mit einer 512-Bit-Schlüsselgröße (Low Grade).

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

Numerische Einträge

4758 PCI Cryptographic Coprocessor
Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann z. B. zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

A

Abstract Syntax Notation One (ASN.1)
Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL
Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll
Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII)
Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI)
Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID
Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI
American National Standards Institute.

Applet
Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Webbrowsers ausgeführt werden kann. Wird auch als Java-Applet bezeichnet.

Art
Siehe Objektart.

ASCII
American National Standard Code for Information Interchange.

ASN.1

Abstract Syntax Notation One.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfasst, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung

Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung

Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B

Base64-Verschlüsselung

Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER)

Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung

Der Prozess, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozess überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER

Basic Encoding Rules.

Berechtigung

Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten

Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser

Siehe Web-Browser.

Browser-Zertifikat

Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Inhaber des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode

Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C

CA

Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie

Bei Tivoli PKI eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem

Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server
Der Server für die CA-Komponente von Tivoli PKI.

CAST-64
Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CA-Zertifikat
Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CCA
IBM Common Cryptographic Architecture.

CDSA
Common Data Security Architecture.

CGI
Common Gateway Interface.

Client
(1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server
Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung
Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA)
IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA)
Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI)
Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Webservern.

CRL
Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Publikationsintervall
Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Publikationen der Zertifikatswiderrufsliste im Directory an.

D

Dämon

Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedingung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, dass der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.

Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck ″Disk And Execution MONitor″ (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES)

Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.

Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL)

Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK

Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER

Distinguished Encoding Rules.

DES

Data Encryption Standard.

Diffie-Hellman

Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digitales Zertifikat

Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Inhabers bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, dass der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Digitale Unterschrift

Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist. Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt. Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht lässt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muss. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digi-

tale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung
Siehe Zertifizierung.

Digital Signature Algorithm (DSA)
Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Directory
Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).
Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im Allgemeinen als ″Blätter″ einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.
Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfasst, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organization Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

```
C=US/O=IBM/OU=Trust/CN=CA1
```

Directory-Server
In Tivoli PKI das IBM Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER)
Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL
Data Storage Library = Datenspeicherbibliothek.

DN
Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK)
Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne
Siehe Sicherheitsdomäne *und* Registrierungsdomäne.

DSA
Digital Signature Algorithm.

E

e-Business
Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce
Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität
Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln
Den Verschlüsselungsprozess rückgängig machen.

Exemplar
Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet
Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP)
Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall
Ein Gateway zwischen Netzen, der den Informationsfluss zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechtigte Verwendung durch externe Personen.

FTP
File Transfer Protocol.

G

Gateway
Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung
Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB)
Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, dass Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechtigt sind.

H

Hierarchie
Die Organisation von Zertifikatsausstellern (CAs) innerhalb einer Trust-Kette. Diese beginnt mit einem selbst unterzeichnenden CA oder übergeordneten Root-CA, der sich an der höchsten Position befindet, und endet mit dem CA, der Zertifikate für Endbenutzer ausstellt.

Höchster CA
Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML
Hypertext Markup Language.

HTTP
Hypertext Transaction Protocol.

HTTP-Server
Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext
Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML)
Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP)
Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

I

ICL
Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis
Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor
Bei Tivoli PKI ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität
Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, dass diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung
Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO)
Eine internationale Organisation, die sich mit der Entwicklung und Veröffentlichung von Standards befasst.

International Telecommunication Union (ITU)
Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur
Siehe Schema.

Internet
Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF)
Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befasst. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet
Ein Netz innerhalb eines Unternehmens, das sich im Allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec
Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO
International Standards Organization.

ITU
International Telecommunication Union.

J

Java
Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java-Anwendung
Ein eigenständiges Programm, das in der Programmiersprache Java geschrieben ist. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet
Siehe Applet. *Gegensatz zu* Java-Anwendung.

Java-Klasse
Eine Einheit mit Java-Programmcode.

Java-Sprache
Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

Java Virtual Machine (JVM)
Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

K

KeyStore (Schlüsselspeicher)
Eine DL zum Speichern von Identitätsnachweisen für Tivoli PKI-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext
Nicht verschlüsselte Daten. *Synonym zu* unverschlüsselter Text.

Klasse

Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie

Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L

LDAP

Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL)

Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M

MAC

Message Authentication Code - Nachrichtenauthentifizierungscode.

MD4

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5

Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

MD2

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

Modulus

In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (n) aus zwei hohen Primzahlen: p und q. Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME)

Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug
Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC)
Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Tivoli PKI werden MAC-Schlüssel für CA- und Prüfkomponenten in den KeyStores gespeichert.

National Security Agency (NSA)
Die offizielle Sicherheitsbehörde der US-Regierung.

NIST
National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS
National Language Support - Unterstützung in der Landessprache.

NSA
National Security Agency.

O

Objekt
Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objektart
Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozess.

Objekt-ID (OID)
Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

ODBC
Open Database Connectivity.

Öffentlicher Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC)
Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI)
Der Name der von ISO genehmigten Computernetzstandards.

OSI
Open Systems Interconnect.

P

PC-Karte
Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im Allgemeinen über eine höhere Kapazität.

PEM
Privacy-Enhanced Mail.

PKCS
Public Key Cryptography Standards.

PKCS #1
Siehe Public Key Cryptography Standards.

PKCS #7
Siehe Public Key Cryptography Standards.

PKCS #10
Siehe Public Key Cryptography Standards.

PKCS #11
Siehe Public Key Cryptography Standards.

PKCS #12
Siehe Public Key Cryptography Standards.

PKI
Public Key Infrastructure.

PKIX
PKI auf X.509v3-Basis.

PKIX Certificate Management Protocol (PKIX CMP)
Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Dies ermöglicht die Unterstützung für zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling).

PKIX CMP
PKIX Certificate Management Protocol.

PKIX-Empfangseinheit
Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Tivoli PKI zu empfangen.

Privacy-Enhanced Mail (PEM)
Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.

Privater Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Protokoll
Eine vereinbarte Konvention für die Kommunikation zwischen Computern.

Protokollierungssubsystem
Bei Tivoli PKI ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.

Proxy-Server
Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server geleitet. Dieser sendet die Anforde-

rung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client
Jeder Client im System, der Prüfereignisse an den Tivoli PKI-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüfprotokoll
Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll
Bei Tivoli PKI eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüf-Server
Ein Tivoli PKI-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfzeichenfolge
Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS)
Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI)
Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechtanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.
PKI stellt öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen zur Verfügung. Er stellt Online-Verzeichnisse bereit, die die öffentlichen Chiffrierschlüssel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.
PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potenzieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA

Registration Authority - Registrierungsstelle.

RA Desktop

Ein Java-Applet, das den RAs eine Grafikschnittstelle für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server

Der Server für die RA-Komponente von Tivoli PKI.

RC2

Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES.
Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muss ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorauszuberechnen.

Regel-Exit

In einer Registrierungsfunktion ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozess.

Registrierter Name (DN)

Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrierung

Bei Tivoli PKI das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsattribut

Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfasst werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrator

Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierungsstelle (RA)

Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, dass die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsdatenbank

Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne

Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungsfunktion eingesetzt wird.

Registrierungsfunktion
Ein Tivoli PKI-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsprozess
Bei Tivoli PKI die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozess werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen. Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsvariable
Siehe Registrierungsattribut.

RSA
Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

Schema
Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel
Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar
Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel
Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheim gehalten. Sender und Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, dass öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Schlüsselsicherung und -wiederherstellung
Diese Funktion von Tivoli PKI ermöglicht das Sichern und Wiederherstellen von Endentitätszertifikaten und der zugehörigen, von Tivoli PKI zertifizierten öffentlichen und privaten Schlüssel. Die Zertifikate und Schlüssel werden in einer PKCS #12-Datei gespeichert. Diese Datei ist kennwortgeschützt. Das Kennwort wird beim Sichern des Zertifikats und der Schlüssel gesetzt.

Secure Electronic Transaction (SET)
Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL)
Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.

Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im Allgemeinen an einem anderen Anschluss (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server

(1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat

Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat *und* Browserzertifikat.

Servlet

Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET

Secure Electronic Transaction.

SGML

Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm)

Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne

Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell

Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Simple Mail Transfer Protocol (SMTP)

Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat

Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card

Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

S/MIME

Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

SMTP

Simple Mail Transfer Protocol.

SSL

Secure Sockets Layer.

Standard Generalized Markup Language (SGML)

Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrischer Schlüssel
Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

Symmetrische Verschlüsselung
Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahren basiert auf dem Schlüssel. Wird dieser öffentlich bekannt gegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheim gehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

T

TCP/IP
Transmission Control Protocol/Internet Protocol.

TP
Trust Policy = Sicherungsregel.

Transaktions-ID
Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Tivoli PKI ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES
Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Tivoli PKI
Eine integrierte IBM Sicherheitslösung, die die Ausstellung, Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

Trust-Kette
Eine Gruppe von Zertifikaten, die aus der gesicherten Hierarchie vom Benutzerzertifikat bis zum Root- oder selbstunterzeichneten Zertifikat besteht.

Tunnel
In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U

Unbestreitbarkeit
Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, dass der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode
Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfasst die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellencode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozessobjekte
Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozessschablone
Eine Gruppe von Unternehmensprozessobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS)
Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen
Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, dass ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen
Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text
Nicht verschlüsselte Daten. *Synonym zu* Klartext.

URL
Uniform Resource Locator - URL-Adresse.

URL-Adresse
Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlussnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8
Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne dass hierbei Informationen verloren gehen.

V

Verkettungsprüfung
Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln
Das Umordnen von Informationen, so dass nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt
Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung
Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne
Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit
Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Vertraulichkeit
Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Virtual Private Network (VPN)
Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung
Bei Tivoli PKI ein Prozess, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Tivoli PKI ein Zertifikat erhalten kann.

VPN
Virtual Private Network.

W

Web-Browser
Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server
Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server
Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Webserver und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW)
Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500
Ein Standard für die Implementierung eines multifunktionalen, verteilten und vervielfältigten Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat
Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.
X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für eine bestimmte Gültigkeitsperiode erstellt werden. Sie können auch auf

anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verlässt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat

Ein weit verbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA)

Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu publizieren. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung

Eine Zusatzfunktion des X.509v3-Zertifikatformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil

Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel

Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL)

Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung

Der Prozess, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel

Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL)

Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

A

Abschnitte, Registrierungsformular 6, 7, 9
Anforderung, Registrierung 3
  auswerten 18
  automatisierte Auswertung 18
  Bearbeitung durch RA 3
  Registrierungsdatenbanksatz 19
  Registrierungsdomäne 19
  Registrierungsformular 17
  über die Registrierungs-Web-Seite 5
  Verarbeitungszyklus 19
  Vorabregistrierung 17
  Web-Browser-Unterstützung 18
Anforderungs-ID 6, 7, 9
Attribute, Datenbanksatz 20
Aussetzen von Zertifikaten
  über die Webseite für die Registrierung 12
Authentifizierung 23

B

Begründung für den Widerruf 29
Beschädigter Schlüssel 29
Browser-Unterstützung 18
Browser-Voraussetzungen 30
Browser-Zertifikat 21
Browser-Zertifikatsanforderung 6

C

CA-Hierarchie 20
CA-Zertifikat 5, 21

D

Datenbanksätze, Registrierung 3, 19
  Attribute 20
  Bearbeitung durch RA 3
DB2 19
Digitale Unterschriften 23
Digitales Zertifikat 21
  Anforderung über die Registrierungs-Web-Seite 5
  Datenbanksätze 19
  erneuerbar 22
  Kategorien 21
  nicht erneuerbar 22
  sichern 14
  Typen 28
Digitales Zertifikat *(Forts.)*
  Verwaltung über die Registrierungs-Web-Seite 11
  wiederherstellen 15
  zur Verwendung der Registrierungsservices 5, 21
Directory-Zugriff 20

E

E-Mail-Benachrichtigung 6, 7, 9, 25
Einheitenzertifikat 7, 22
Erläuterungen, Abschnitte 17
Erneuerbares Zertifikat 22
Erneuerbarkeit 22
Erneuerung
  über die Webseite für die Registrierung 12

F

Felder des Registrierungsformulars 25

G

Gegenseitige Zertifizierung 20
Geschäftsprozessvariablen 22
Gesicherte Anwendungen 23
Gesicherte Ressourcen 3, 23
Gültigkeitszeitraum 28

I

Identifikationsprüfungsantwort 6, 7, 9, 11, 25
Informationen zur Vorgehensweise, Abschnitte 5
Inhalt des Handbuchs vii
Internet Explorer - Browser-Zertifikat 6

K

Konventionen ix
Kundenunterstützung ix

L

LDAP-Protokoll 20

N

Netscape - Browser-Zertifikat 6
Nicht erneuerbares Zertifikat 22

P

PKCS #10-Anforderung für Zertifikate 22, 25
PKCS #12-Datei sichern 14
PKCS #12-Datei wiederherstellen 15, 23
PKIX-kompatible Anwendung 9, 21
Protokoll, Directory-Zugriff 20
Protokolle 21

R

RA 18
RA Desktop 17, 19
Referenzinformationen, Abschnitte 25
Registrator 17, 18, 19
Registrierter Name 20
Registrierung 18
  automatisiert 18
  Bedarf 3
  Regeln 19
  Systemvoraussetzungen 30
  über die Registrierungs-Web-Seite 5
  Web-Browser-Unterstützung 18
Registrierungs-Web-Seite 3, 5
  Anforderungs-ID 6, 7, 9
  Anforderungsstatus überprüfen 11
  CA-Zertifikat 21
  Felder des Registrierungsformulars 25
  Registrierungstypen 17
  Szenario für die Vorabregistrierung 17
  URL 5
  Zugriff 5
Registrierungsanforderung 3
  auswerten 18
  automatisierte Auswertung 18
  Bearbeitung durch RA 3
  Registrierungsdatenbanksatz 19
  Registrierungsdomäne 19
  Registrierungsformular 17
  über die Registrierungs-Web-Seite 5
  Verarbeitungszyklus 19
  Vorabregistrierung 17
  Web-Browser-Unterstützung 18
Registrierungsbeschränkungen 25
Registrierungsdatenbanksätze 3, 19
  Attribute 20
Registrierungsdatenbanksätze *(Forts.)*
  Bearbeitung durch RA 3
Registrierungsdomäne 19
Registrierungsformularfelder 25
Registrierungsstelle 3, 18

S

Schlüssel, beschädigt 29
Schlüsselsicherung anfordern 14
Schlüsselsicherungsanforderung, Webseite 14
Schlüsselwiederherstellung 23
Schlüsselwiederherstellung anfordern 15
Schlüsselwiederherstellungsanforderung, Webseite 15
Server-Zertifikat 7, 22
Sicherung und Wiederherstellung von Schlüsseln 23
Sicherungsanforderung ausgeben für Schlüssel 14
Systemvoraussetzungen
  Browser-Registrierung 30

T

Tivoli
  Kundenunterstützung ix
  Sicherheitsverwaltung - Webinformationen ix
Tivoli PKI
  Webinformationen ix
Tivoli PKI, Zusammenfassung 1
Typ des Zertifikats 28

U

Übersicht 3
Unternehmensregeln 18
Unterstützung für Tivoli-Kunden ix
Unterzeichnen von Dateien 23
URL
  Registrierungs-Web-Seite 5
  Registrierungsdomäne 19
  Schlüsselsicherungsanforderung 14
  Schlüsselwiederherstellungsanforderung 15

V

Veröffentlichungen
  Tivoli-Sicherheitsprodukte ix
Verwendungszweck des Zertifikats 28
Vorabregistrierung 17
  Anforderungsstatus überprüfen 11
  Szenario für Tasks 17
Vorabregistrierungsdatei 11
Vorwort vii

W

Web-Browser-Unterstützung 17, 18
Web-Seite, Registrierung 3, 5
  Anforderungs-ID 6, 7, 9
  Anforderungsstatus überprüfen 11
  CA-Zertifikat 21
  Felder des Registrierungsformulars 25
  Registrierungstypen 17
  Szenario für die Vorabregistrierung 17
  URL 5
  Zugriff 5
Website für
  Sicherheitsverwaltungsinformationen ix
  Tivoli-Kundenunterstützung ix
  Tivoli Public Key Infrastructure ix
  Tivoli-Sicherheitsprodukte ix
Widerruf
  Begründung 29
  über die Webseite für die Registrierung 13
Wiederherstellung von Schlüsseln 23
Wiederherstellungsanforderung ausgeben für Schlüssel 15

X

X.509v3-Zertifikatserweiterungen 22

Z

Zertifikat 21
  Anforderung über die Registrierungs-Web-Seite 5
  Datenbanksätze 19
  erneuerbar 22
  Kategorien 21
  nicht erneuerbar 22
  sichern 14
  Typen 28
  Verwaltung über die Registrierungs-Web-Seite 11
  wiederherstellen 15
  zur Verwendung der Registrierungsservices 5, 21
Zertifikatsaussteller (CA) 3, 20
Zertifikatserweiterungen 22
Zertifikatstypen 28
Zertifikatsverarbeitungszyklus 19, 22
Zertifikatsverwaltung (im Web) 11
  Anforderung für Browser 6
  Anforderung für Server-Einheit 7
  aussetzen 12
  erneuern 12
  Vorabregistrierung 9
  widerrufen 13
Zertifikatswiderrufsliste (CRL) 20
Zertifizierung 20
  gegenseitige Zertifizierung 20
  Hierarchie 20
Zielgruppe vii
Zugriffssteuerungsliste (ACL) 23
Zusammenfassung
  verwendete Konventionen ix

SH12-2978-02